SPECIAL SUPPLEMENT BY
Enterprise CHANNELS MEA

VOLUME 08 | ISSUE 01 | **JANUARY 2026**

CYBER SENTINELS

Loubna Imenchal
Regional Director for Middle East, Türkiye, Central Asia and Africa at Axis Communications

The age of intelligent security

Axis Communications is redefining what physical security means in an increasingly digital and connected world.

Held under the patronage of **H.H. Sheikh Mansoor bin Mohammed bin Rashid Al Maktoum,**
Chairman of Dubai Ports and Borders Security Council

intersec

12 – 14 January 2026
Dubai World Trade Centre

The world's premier event for Security, Safety and Fire Protection.

50,000+
Visitors

140+
Visiting Countries

1,400+
Exhibitors

60+
Exhibiting Countries

SCAN THE QR CODE TO GET YOUR COMPLIMENTARY VISITOR PASS

intersec.ae.messefrankfurt.com intersec@uae.messefrankfurt.com

messe frankfurt

EDITORIAL

Physical security enters the enterprise era

JEEVAN THANKAPPAN
jeevan@gcemediagroup.com

Physical security is undergoing one of the most significant transformations in its history. What was once a function focused almost exclusively on protection and loss prevention is rapidly evolving into a strategic, data-driven capability that supports broader business outcomes. At the centre of this shift is a powerful force reshaping the industry: the growing influence of IT.

According to the latest Genetec State of Physical Security Report, physical security leaders around the world are increasingly positioning their systems as enterprise platforms rather than standalone safeguards. Based on insights from more than 7,300 professionals globally, the report paints a clear picture of security teams working more closely with IT, operations, facilities, and business leaders to deliver operational awareness, resilience, and smarter decision-making.

This convergence is not accidental. As organisations digitise physical environments, security systems are becoming rich sources of data. Video, access control, sensors, and analytics are now feeding intelligence into enterprise workflows, helping organisations optimise operations, improve safety, and respond faster to real-world events. In this new model, physical security is no longer just about stopping bad things from happening; it is about enabling better outcomes across the business.

IT's influence is also reshaping how infrastructure decisions are made. Hybrid cloud models are now firmly established as the preferred approach, combining on-premises control with cloud-based flexibility. Automatic updates, easier deployment, and simplified maintenance are driving adoption, while IT teams help ensure security systems meet enterprise standards for reliability, cybersecurity, and lifecycle management.

Artificial intelligence is another area where IT and physical security priorities are converging. For the first time, AI now ranks alongside video surveillance and access control as a top project priority for 2026. Interest in AI adoption has more than doubled year over year, driven by practical use cases such as alarm triage, faster investigations, and noise reduction. At the same time, concerns around data use and transparency remain high, reinforcing the need for IT-led governance and vendor accountability.

As physical security becomes deeply embedded in enterprise ecosystems, its future will be shaped as much by IT strategy as by traditional security needs. The organisations that succeed will be those that embrace this convergence, treating physical security not as an isolated function, but as a core pillar of intelligent, resilient, and data-driven operations.

CYBER **SENTINELS**

PUBLISHER
TUSHAR SAHOO
tushar@gecmediagroup.com

CO-FOUNDER & CEO
RONAK SAMANTARAY
ronak@gecmediagroup.com

EXECUTIVE DIRECTOR
Akashdeep Singh: akashdeep@gecmediagroup.com

MANAGING EDITORS
Jeevan Thankappan: jeevan@gecmediagroup.com
Arun Shankar: arun@gecmediagroup.com

ASSISTANT EDITOR
Rehisha: rehishap@gecmediagroup.com

CHIEF STRATEGY OFFICER
Anushree Dixit: anushree@gecmediagroup.com

CHIEF COMMERCIAL OFFICER
Richa S: richa@gecmediagroup.com

DIGITAL MARKETING HEAD
Santosh Pania: santosh@gecmediagroup.com

COMMUNICATIONS LEAD GCC

IT MANAGER
Vijay Bakshi: vijay@gecmediagroup.com

PRODUCTION
S.M. MUZAMIL: muzamil@gecmediagroup.com
Mohammed Kagzi, Abdullah A. Hameed

CREATIVE LEAD
Ajay Arya

SR. DESIGNER
Shadab Khan

CONTENT WRITER
Kumari Ambika

DESIGNED BY
THE C2S
DESIGN • MARCOM • BRANDING

SUBSCRIPTIONS
info@gecmediagroup.com

PRINTED BY
Al Ghurair Printing & Publishing LLC.
Masafi Compound, Satwa, P.O.Box: 5613, Dubai, UAE

GEC Global Enterprise Connect

(UAE) Office No #115
First Floor , G2 Building
Dubai Production City
Dubai, United Arab Emirates
Phone : +971 4 564 8684

(USA) 31 FOXTAIL LAN,
MONMOUTH JUNCTION,
NJ - 08852
UNITED STATES OF AMERICA
Phone :+ 1 732 794 5918

A PUBLICATION LICENSED BY
International Media Production Zone, Dubai, UAE

GEC Global Enterprise Connect

2026 EVENT CALENDAR

JAN

- 26 - GLOBAL SECURITY SYMPOSIUM - PAKISTAN
- 27 - FORESIGHT 2026

FEB

- 05 - CLOUD SUMMIT - UAE
- 12 - CLOUD SUMMIT - KSA
- 26 - GEC IFTAR

MAR

- TBD - IFTAR

APR

- 05 - WORLD CIO 200 SUMMIT - MOROCCO
- 12 - GEC AWARDS - KSA
- 14 - GEC AI SUMMIT
- 15 - GLOBAL SECURITY SYMPOSIUM - UAE
- 20 - GLOBAL SECURITY SYMPOSIUM - KSA
- 22 - WORLD CIO 200 SUMMIT - HONG KONG
- 23 - GLOBAL SECURITY SYMPOSIUM - QATAR
- 29 - WORLD CIO 200 SUMMIT - PHILIPPINES

MAY

- 08 - WORLD CIO 200 SUMMIT - SINGAPORE
- 12 - WORLD CIO 200 SUMMIT - MALAYSIA
- 14 - WORLD CIO 200 SUMMIT - INDONESIA
- 20- WORLD CIO 200 SUMMIT - USA
- 20 - WORLD CIO 200 SUMMIT NIGERIA - GHANA
- 22 - WORLD CIO 200 SUMMIT AFRICA - KENYA

JUN

- 11 - WORLD CIO 200 SUMMIT - UAE
- 17 - WORLD CIO 200 SUMMIT - QATAR
- 18 - WORLD CIO 200 SUMMIT - OMAN
- 18 - WORLD CIO 200 SUMMIT - GERMANY
- 23 - WORLD CIO 200 SUMMIT - BAHRAIN

JUL

- 08 - WORLD CIO 200 SUMMIT - KSA
- 16 - WORLD CIO 200 SUMMIT - LONDON
- 17 - CPCA - KENYA

AUG

- 06 - WORLD CIO 200 SUMMIT - SOUTH AFRICA
- 19 - CLOUD SUMMIT - KENYA
- 28 - WOMEN LEADERSHIP SYMPOSIUM

SEP

- 15 - WORLD CIO 200 SUMMIT - GRAND FINALE

OCT

- 06 - CPCA - UAE
- 08 - CPCA - KSA
- 08 - GEC AI SUMMIT
- 26 - CLOUD SUMMIT - PHILIPPINES
- 27 - CLOUD SUMMIT - INDONESIA
- 29 - CLOUD SUMMIT - MALAYSIA

NOV

- 05 - GEC VERTICAL DAYS

DEC

- 07 - GEC AWARDS 2026

CONTENTS

JANUARY 2026

Morey J. Haber
Chief Security Advisor at BeyondTrust

BeyondTrust experts reveal top cybersecurity predictions for 2026 and beyond

BeyondTrust, global leader in identity security protecting Paths to Privilege, has announced its top cybersecurity predictions for 2026 and beyond, identifying the trends that will redefine how organizations protect identities, secure data, and prepare for a rapidly evolving threat landscape.

The annual forecast, developed by leading BeyondTrust experts, Morey J. Haber, Chief Security Advisor; Christopher Hills, Chief Security Strategist; and James Maude, Field Chief Technology Officer, highlights key developments expected in the next year, as well as those on the horizon expected to redefine security strategies over the next five years and beyond.

"Cybersecurity has always been a forward-looking discipline," said Morey J. Haber, Chief Security Advisor at BeyondTrust. "By anticipating where technology, threat actors, and regulation are heading, we can better protect our customers and help the industry prepare for what's next. Looking ahead allows us to adapt faster and turn insight into proactive security action."

OPSWAT–SANS survey: 21.5% of organisations hit by ICS/OT cyber incidents

Matt Wiseman
Director of Product Marketing at OPSWAT

OPSWAT, a global leader in critical infrastructure protection (CIP) cybersecurity solutions, has announced findings from the SANS Institute's The State of ICS/OT Cybersecurity 2025 reportsponsored by OPSWAT.

"This year's findings show that while progress is being made, the industry still faces significant challenges in securing converged environments," said Jason Christopher, SANS Institute, author of the report. "Organisations must prioritize visibility and segmentation to mitigate these risks effectively."

"Our earlier research with the SANS Institute showed that most organisations dedicate less than 25% of their security budgets to OT," said Matt Wiseman, Director of Product Marketing at OPSWAT. "The new findings make it clear that increased spending alone is not enough. The priority now is smarter investment in the controls that matter most for safety and uptime: segmentation, secure remote access, and scanning inbound files and devices before they reach the operational environment. OT security requires an integrated approach that closes the gaps attackers continue to exploit."

Axis Communications to unveil intelligent security tech at Intersec 2026

Loubna Imenchal
Regional Director for Middle East, Türkiye, Central Asia and Africa at Axis Communications

The global security landscape is undergoing a profound transformation – shifting rapidly from traditional, reactive surveillance to a new era defined by intelligent, AI-powered and data-driven security systems. As the world's leading provider of network surveillance and security solutions, Axis Communications will take center stage at Intersec Dubai 2026, demonstrating cutting-edge technologies that continue to shape the future of safety, security, efficiency, and smart operations across the world's most critical industries.

Held under the patronage of HH Sheikh Mansoor Bin Mohammed bin Rashid Al Maktoum, the 27th edition of Intersec will run from 12 to 14 January 2026 at Dubai World Trade Centre. As one of the most influential global platforms for security and safety, the event will bring together experts, government leaders, technology partners and industry innovators to explore the future of intelligent protection and cross-sector collaboration.

For Axis, participating in Intersec is more than a showcase – it is a strategic opportunity to demonstrate the real-world impact of innovation and reaffirm its commitment to solving the industry's most complex challenges at the edge.

"Across the Middle East and Africa, we are seeing a fundamental shift in how organizations view surveillance. It is no longer just a safeguard – it is becoming a core driver of business efficiency, resilience and informed decision-making," said Loubna Imenchal, Managing Director for Middle East, Türkiye, Central Asia and Africa at Axis Communications. "At Intersec, we will showcase how intelligence at the edge is redefining what's possible for security, operations and smart environments."

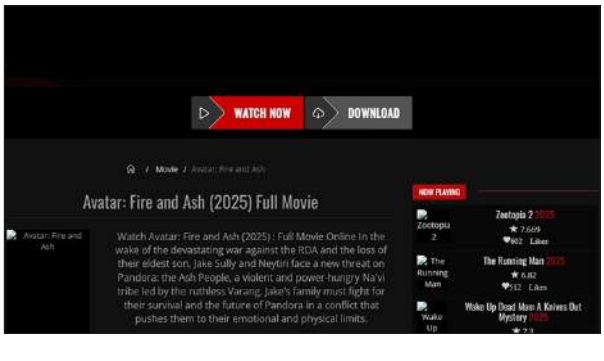
Kaspersky identifies global scam activity linked to the release of Avatar 3

The premiere of Avatar 3 has taken place in several countries and has been accompanied by a noticeable increase in online interest. Amid the heightened attention surrounding the release, Kaspersky experts have identified an increase in cyber-scam campaigns that exploit the movie's launch and users' desire to watch it online. The fraudulent websites target users across multiple regions, indicating attempts by attackers to reach a global audience.

The scam operates as follows: cybercriminals create suspicious websites that offer online access to the Avatar 3 movie. Attackers place particular emphasis on localization, publishing the sites in multiple languages to attract users from different countries. However, the translations are often poorly executed and contain grammatical errors and inconsistencies, which may serve as indicators of fraudulent activity.

When users attempt to start the video, they are presented with a fake media player and prompted to register in order to obtain "full" or "unlimited" access to the film. As part of the registration process, users are asked to provide personal information, including an email address and mobile phone number.

"Cybercriminals consistently exploit major movie premieres to capture users' attention and increase the effectiveness of their schemes.



We advise accessing films only through official platforms and exercising caution when encountering websites that request personal or payment information. It is also important to use reliable security solutions to protect all devices, including mobiles," comments Olga Altukhova, Senior web content analyst at Kaspersky.

BJ Jenkins
President, Palo Alto Networks

Palo Alto Networks and Google Cloud partner to secure cloud and AI initiatives

As enterprises race to harness the transformative power of agentic AI and cloud computing, Palo Alto Networks and Google Cloud announced a significant expansion of their strategic partnership to enable the secure development and deployment of AI solutions and provide a trusted foundation that helps organizations harness the full potential of AI with confidence. The collaboration combines Google Cloud's leading AI and infrastructure capabilities with Prisma AIRS, Palo Alto Networks comprehensive AI security platform, to secure the next generation of digital business.

Palo Alto Networks recent State of Cloud Report, released in December 2025, found that customers are dramatically expanding their use of cloud infrastructure to support new AI applications and services, while also noting that 99% of respondents experienced at least one attack on their AI infrastructure over the last year.

BJ Jenkins, President, Palo Alto Networks said, "Every board is asking how to harness AI's power without exposing the business to new threats. This partnership answers that question. We're removing the friction between security and development, providing a unified platform where the most advanced security is simply a native part of building what's next. Together with Google, we are embedding our AI-powered security deep into the Google Cloud fabric, turning the platform itself into a proactive defense system."

Group-IB and VAS Integrated Solutions sign MoU to boost cybersecurity cooperation in the Kingdom

Group-IB, a leading creator of cybersecurity technologies to investigate, prevent, and fight digital crime, and VAS Integrated Solutions, a value-added distributor (VAD) of leading brands, providing integrated IT solutions to the various market verticals, have signed a Memorandum of Understanding (MoU) to explore strategic cooperation and future channel-led expansion opportunities across the Kingdom of Saudi Arabia.

The agreement lays the groundwork for a strategic partnership that will enhance knowledge-sharing, innovation, and the development of solutions tailored to address the region's rapidly evolving digital threats.

The MoU was signed by Mohammad Flaifel, Regional Sales Director of KSA and Türkiye at Group-IB, and Bilal Abdulrahman, Country Manager, KSA & GCC at VAS Integrated Solutions, on the sidelines of Black Hat MEA, reflecting a shared vision to support the growth of Saudi Arabia's cybersecurity ecosystem through strong local partnerships.

The cooperation establishes a framework for joint market development, partner enablement, and awareness initiatives, grounded in Group-IB's adversary-centric and predictive approach to cyber threat and fraud intelligence. Through its Digital Crime Resistance Center (DCRC) model, Group-IB combines on-the-ground expertise in the Middle East and Africa with its global threat intelligence, and investigative capabilities, enabling organizations in Saudi Arabia to anticipate, prevent, and respond to complex cyber and fraud threats with local context and rapid response.

ServiceNow to acquire Armis to expand cyber exposure security across IT, OT, and medical devices

ServiceNow, the AI control tower for business reinvention, has entered into an agreement to acquire Armis for $7.75 billion in cash. Armis, a leader in cyber exposure management and cyber-physical security, manages cyber risk across the full attack surface in IT, operational technology (OT), medical devices, and other environments for companies, governments, and critical infrastructure worldwide. The acquisition will expand ServiceNow's security workflow offerings and advance AI-native, proactive cybersecurity and vulnerability response across all connected devices. Together, ServiceNow and Armis will create a unified, end-to-end security exposure and operations stack that can see, decide, and act across the entire technology footprint by connecting real-time asset discovery, threat intelligence, and risk prioritisation with automated remediation and response workflows.

Amit Zavery
President, Chief Operating Officer, and Chief Product Officer at ServiceNow

Security continues to be the number one priority for CEOs as organizations navigate increased adoption of AI. Worldwide end-user spending on information security is projected to increase 12.5% in 2026 to $240 billion, with rising threats and the expanding use of AI and generative AI being the key growth drivers. As rapid AI adoption expands the attack surface for organizations, real-time visibility into vulnerabilities and actionable insights for what to fix first are critical to minimize risk and strengthen security posture.

CrowdStrike, AWS and NVIDIA select 35 startups for 2026 cybersecurity accelerator

CrowdStrike announced the 35 startups selected for its third annual Cybersecurity Startup Accelerator with Amazon Web Services (AWS) and NVIDIA through its Inception program, fueling the next generation of AI-driven cloud security innovation. Chosen from hundreds of global applicants, the elite group was selected for the strength of their innovation, potential to make market impact, and caliber of their teams.

The free, eight-week program runs from today through March 3, 2026, providing startups with mentorship, technical expertise, funding and go-to-market support, along with access to top cybersecurity experts and global visibility across partner ecosystems.

The program will culminate in a final pitch day for five finalists during the RSA Conference in San Francisco on March 24, 2026, where an expert panel will select one innovation award winner, with potential for investment from the CrowdStrike Falcon Fund.

Daniel Bernard
Chief Business Officer at CrowdStrike

"The Cybersecurity Startup Accelerator has become a launchpad for the next era of AI-driven security innovators," said Daniel Bernard, Chief Business Officer at CrowdStrike. "This year's cohort reflects a global movement: founders building cloud- and identity-first defenses that put security teams ahead of the speed and scale of AI-emboldened adversaries. With AWS and NVIDIA, we're creating community and growing "the crowd," giving these startups the opportunity to turn breakthrough ideas into market-shaping technologies, and push the industry forward."

Edgard Capdevielle
CEO, Nozomi Networks

Gartner: Nozomi Networks named AI leader in cyber-physical security

Nozomi Networks, offering solutions in OT, IoT and CPS security, announced it has been recognized as the company to beat for AI in Cyber-Physical Systems Security in the Gartner report for AI Vendor Races.

According to Gartner, "Native and embedded CPS capabilities and whole life cycle coverage out Nozomi at the head of the pack." The report notes, "Nozomi's early approach of embedding machine learning (ML) capabilities natively during the earliest stages of product development in 2013 has given its Nozomi CPS security product an operational head start in enabling AI to support CPS discovery, analysis and alerting capabilities."

"We are proud to be recognized by Gartner Research as the Company to beat for AI in cyber-physical systems protection," said Nozomi Networks CEO Edgard Capdevielle. "We believe this recognition is a testament to our team's dedication to safeguarding the world's most essential systems and our ongoing commitment to innovation in AI-driven cybersecurity."

Refined in-house for more than a decade, Nozomi Networks' AI-powered platform empowers organizations to proactively detect, respond to and mitigate cyber threats targeting industrial and critical infrastructure. Nozomi's AI engine uses a variety of techniques to enrich asset profiles, baseline normal behavior, raise issues and provide actionable to deliver robust visibility and security for complex cyber-physical systems across energy, manufacturing, transportation healthcare and other sectors.

CyberKnight teams up with Hexnode to boost endpoint security

CyberKnight, a leading value-added distributor (VAD) specializing in zero trust security, announced a strategic partnership with Hexnode, the global leader in Unified Endpoint Management (UEM). As organizations across the MEA (Middle East and Africa) accelerate digital transformation and hybrid work adoption, the rising complexity of managing endpoints and applications has created an urgent demand for simplified, scalable, and secure management solutions.

According to Gartner's Market Guide for Unified Endpoint Management, Hexnode has consistently received honourable mentions, while also cited as a Notable Vendor in the Forrester Landscape Report for Unified Endpoint Management Q3 2025 for its intuitive interface, rapid deployment capabilities, and robust security integrations. With a user base spanning worldwide, Hexnode empowers enterprises to secure, monitor, and manage every device in their ecosystem—across mobile, desktop, and IoT environments—from a single, unified platform.

The partnership between CyberKnight and Hexnode aims to tackle one of the region's most pressing cybersecurity challenges: gaining centralized visibility and control over an increasingly diverse device landscape. By combining Hexnode's award-winning UEM technology with CyberKnight's Zero Trust Security framework and deep regional expertise, the two companies will deliver holistic endpoint protection and compliance solutions to enterprise customers across sectors such as finance, education, healthcare, and government.

Genetec predicts top physical security trends for 2026

Genetec, the global leader in enterprise physical security software, predicts four key trends that will shape physical security strategies in 2026, from flexible cloud deployment and intelligent automation to modernized access control and more connected, unified security operations. Against a backdrop of rising cyber-physical risk and growing data volumes, these trends are set to influence how organizations in the Middle East and beyond invest in and manage their security environments.

1. Choice and flexibility will define the next phase of cloud adoption

Organizations will prioritize solutions that offer deployment flexibility and scalability. They will then choose the environment that best supports their operational needs, whether it's on-premises, in the cloud, or a hybrid approach.

2. AI moves from hype to intelligent automation

In 2026, the conversation will shift from AI and LLM hype to practical, outcome-driven Intelligent Automation (IA) solutions that streamline workflows, improve accuracy, and enable faster, smarter decisions.

3. Access control modernization will accelerate

Access control will remain a top priority as organizations modernize legacy systems and focus on maximizing ROI. The value of access control is expanding well beyond locking and unlocking doors to deliver measurable business outcomes, such as energy efficiency, occupancy management, and operational insights.

4. Connected systems will bring intelligence and efficiency to security operations

Over the next year, the number of connected devices will continue to surge as organizations integrate IoT sensors, building systems, and smart devices into unified security and operations platforms.

As the landscape grows more complex, organizations will seek guidance on how to deploy the right technologies and manage them effectively.

Cisco outlines key AI security strategies as adoption grows in the Middle East

Fady Younes
Managing Director for Cybersecurity at Cisco Middle East, Africa, Türkiye, Romania and CIS

Cisco highlights four priority focus areas organizations should consider to secure AI applications as they scale adoption. The guidance outlines how security teams can adapt proven application security practices to AI, helping organizations across the Middle East manage emerging risks and maintain digital trust.

As AI adoption scales across the Middle East, including government, financial services, energy, and critical infrastructure, CISOs and IT leaders are under pressure to secure AI applications across the full lifecycle, from the data they rely on to the models they deploy.

Fady Younes, Managing Director for Cybersecurity at Cisco Middle East, Africa, Türkiye, Romania and CIS, commented: "As AI adoption accelerates across the region organizations are moving quickly from pilots to production, and that shift changes the risk profile. Securing AI applications requires looking beyond traditional application controls to protect the full AI lifecycle, from the data and third-party components feeding models to how those models behave in real world use. By applying familiar security principles in AI specific ways, organizations in the Middle East can scale innovation with confidence while reducing risks such as prompt injection and sensitive data leakage."

Craig Coogan
CTO & VP, Product & Strategy, Access Network Solutions, CommScope

CommScope launches secure boot solution for TI Arm-based AM6x processors

CommScope, a global leader in network connectivity, announced a fully tested, out-of-the-box bootloader signing solution for the Texas Instruments' (TI) Arm-based AM6x processor family. Built on CommScope's PRiSM (Permission Rights Signing Manager) platform, this solution is simple and easy to integrate with the TI image build process; and it ensures robust key protection using a FIPS-certified Hardware Security Module (HSM) and centralised key lifecycle management. The solution delivers a production-ready path to secure boot adoption—streamlining Continuous Integration/Continuous Delivery (CI/CD) and meeting cybersecurity mandates without requiring teams to build and manage their own cryptographic infrastructure.

Bootloader security is a critical foundation for ensuring device integrity because it determines whether firmware can be trusted before executing it. This function requires protecting the private signing key used to authenticate firmware; if that key is compromised, even secure boot mechanisms can be bypassed. CommScope's solution helps manufacturers safeguard this key with hardware-backed security and controlled access, offering a clear, auditable path to meet emerging cybersecurity mandates, including the European Union's Cyber Resilience Act (CRA) as well as other regional and industry-specific standards.

"Security should never be a barrier to product innovation," said Craig Coogan, CTO & VP, Product & Strategy, Access Network Solutions, CommScope. "By collaborating with TI, we help device makers simplify secure boot adoption, reduce development friction, and deliver trusted products into regulated markets with confidence. We handle the underlying complexity so device manufacturers can focus on what they do best to improve productivity, streamline development, and strengthen security outcomes."

SANS Institute partners with UAE Cybersecurity Council to strengthen cyber capabilities for the quantum era

From L-R, Ned Baltagi at SANS Institute with His Excellency Dr. Mohammed Alkuwaiti, Head of the UAE Cyber Security Council

SANS Institute, the global leader in cybersecurity training and certifications, announced a landmark strategic partnership with the UAE Cybersecurity Council to advance the nation's cybersecurity readiness and reinforce the UAEs long-term vision for a secure and resilient digital future. The agreement was formalised during CyberQ 2025 in the presence of His Excellency Dr. Mohammed Alkuwaiti, Head of the UAE Cyber Security Council, and Ned Baltagi, Managing Director – Middle East, Turkey and Africa at SANS Institute.

This strategic partnership unites both entities under a shared commitment to strengthen national cybersecurity capabilities through cooperation across critical ICT and cybersecurity domains. The primary focus is to elevate national preparedness in cyberattack prevention, detection, and response, while deepening knowledge of emerging threats, and enhancing technical expertise across the workforce. As part of this initiative, SANS Institute conducted a workshop on 'Cybersecurity in the Quantum Era.' Going forward, the company will introduce future-oriented training programmes in Secure AI and Quantum Security that will equip cybersecurity professionals to navigate next-generation technological risks.

Ned Baltagi, Managing Director – Middle East, Turkey and Africa, SANS Institute, said, "We are honoured to collaborate with the UAE Cybersecurity Council on this important national mission to enhance cyber resilience and support the country's digital transformation agenda. This MoU marks a significant milestone in our shared efforts to empower cybersecurity professionals with advanced expertise and future-ready skills. Through initiatives such as the Quantum Security program and our ongoing capability-building activities, we are committed to supporting the UAE as it strengthens its position as a global leader in cybersecurity."

Sophos XDR delivers 100% detection coverage in the latest MITRE ATT&CK Evaluation

Simon Reed
Chief Research and Scientific Officer, Sophos

Sophos, a global leader of innovative security solutions for defeating cyberattacks, announced its best-ever results in the MITRE ATT&CK Enterprise 2025 Evaluation. Sophos XDR detected 100% of adversary behaviors (sub-steps)1 across two complex attack scenarios: Scattered Spider, which Sophos X-Ops tracks as GOLD HARVEST, a financially motivated cybercriminal collective, and Mustang Panda, which Sophos X-Ops tracks as BRONZE PRESIDENT, a People's Republic of China (PRC) espionage group. The Scattered Spider scenario included activity across Windows, Linux, and AWS cloud environments, and the Mustang Panda scenario focused on Windows only. Further, Sophos achieved the highest-possible "Technique"-level rating for 86 out of 90 total sub-steps in the evaluation, by generating high-fidelity detections with details on execution, impact, and adversary behavior, providing clear who, what, when, where, how, and why insights.

"Scattered Spider and Mustang Panda represent distinct threat profiles that challenge defenders in very different ways," said Simon Reed, Chief Research And Scientific Officer, Sophos. "achieving full detection coverage against both validates the accuracy and depth of Sophos' analytics and demonstrates how the company's ai-native xdr platform converts complex telemetry into clear, actionable intelligence, helping security teams detect, understand, and stop advanced attacks with confidence. Sophos' consistently strong performance in these rigorous evaluations underscores the power and precision of our threat detection and response capabilities, and our commitment to stopping the world's most sophisticated cyberthreats. over the five years that Sophos has participated in att&ck evaluations, we have continually invested in strengthening our platform, and that investment has translated into stronger results year after year - both in the evaluations, and in the security outcomes we deliver for our customers."

Hexnode expands into UAE's endpoint security space with Hexnode XDR

Hexnode, the enterprise software division of Mitsogo, released Hexnode XDR, its extended detection and response platform, marking a significant step in its effort to strengthen cyber resilience across organisations in the UAE.

As the UAE continues its rapid digital transformation, it has also become a prime target for sophisticated cyber threats. The nation regularly confronts a surge of malicious activity, with security authorities blocking more than 200,000 cyberattacks every day across critical infrastructure and business environments.

"As digital adoption accelerates across the UAE, security teams are under pressure to respond faster and with better context," said Tim Bell, VP of Sales, EMEA & APJ. "Hexnode XDR helps bring structure and context to endpoint security operations, allowing organisations to respond with greater clarity and confidence."

Hexnode XDR reimagines the XDR experience with usability at its core. Its clean, structured dashboard unifies endpoints, alerts and vulnerabilities into a single view, simplifying how IT teams assess and respond to threats.

Hexnode XDR integrates seamlessly with Hexnode UEM, creating a single connected environment for endpoint management and security. This unified approach reduces tool sprawl and shortens response time.

A better **posture**

Close on the heels of its acquisition of Securiti AI, Anand Eswaran, CEO of Veeam, shared his perspective on why traditional approaches to data security are increasingly unfit for today's AI-driven reality, and how the combination of Veeam and Securiti AI is designed to secure, govern, and recover data at unprecedented speed and scale.

When Veeam first began evaluating the data security landscape, Eswaran observed a market in the midst of rapid consolidation. Many security vendors were attempting to integrate data security into their broader platforms. Established players such as CrowdStrike and Palo Alto Networks were acquiring data security posture management (DSPM) companies, while organisations rooted in data resilience were also pursuing similar acquisitions to expand their portfolios.

Despite this activity, Eswaran felt that most of these efforts were missing something fundamental. What stood out was not a lack of technology, but a lack of a holistic approach. By holistic, he refers to the need to protect and govern data across the entire data estate, spanning production environments, backup systems, and the way data ultimately feeds AI pipelines. In practice, however, many organisations were deploying DSPM solutions in a fragmented manner, focusing only on production data or only on backup data. That separation, he argues, represents a structural flaw at a time when data environments are becoming more interconnected and dynamic.

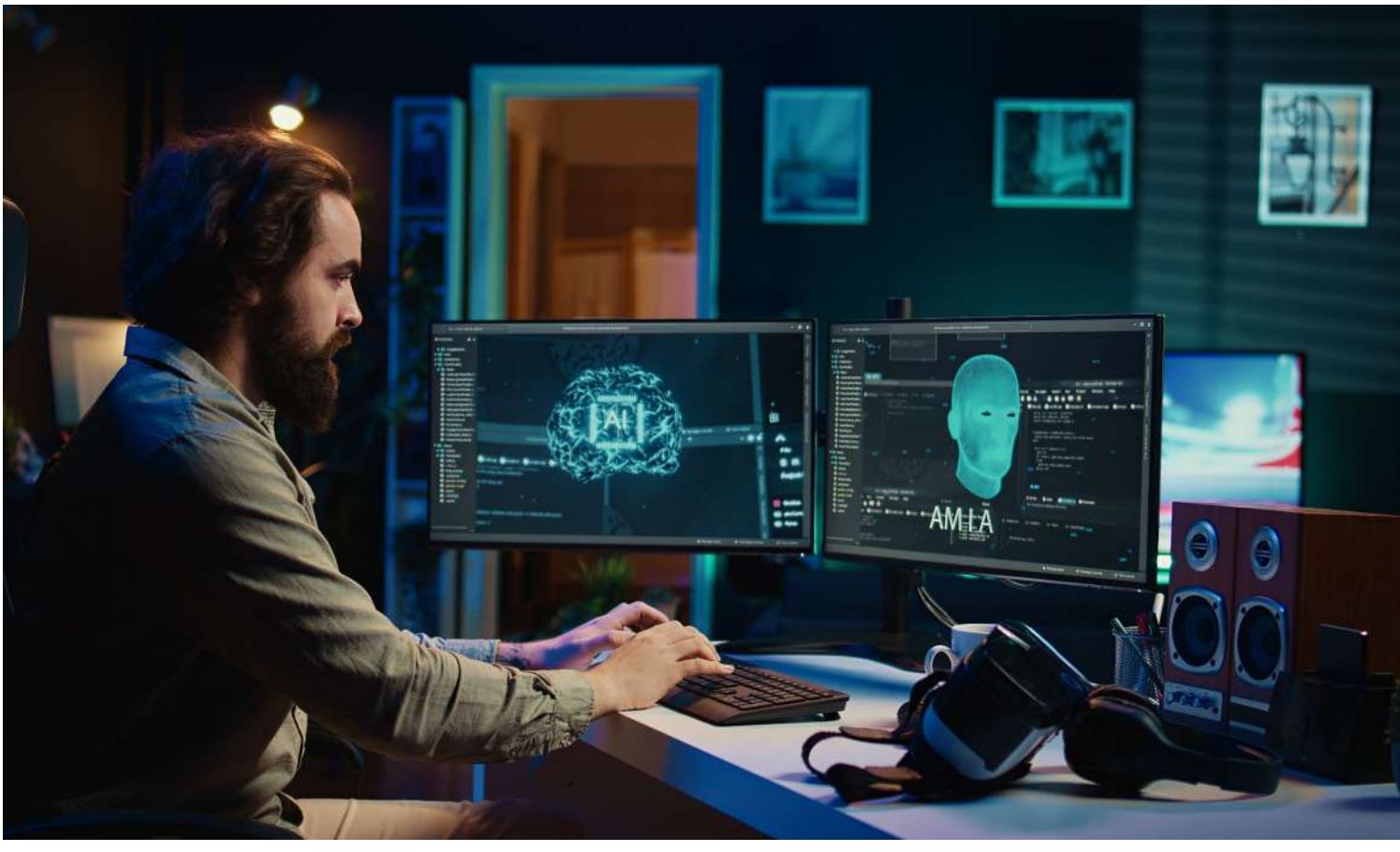
A second major gap quickly became apparent: the absence of deep, integrated privacy, compliance, and governance controls. These capabilities are no longer optional. They are foundational requirements, particularly as regulatory scrutiny increases and data is reused for analytics and AI. "Yet most DSPM solutions treat privacy and governance as secondary layers rather than core design principles, leaving organisations to stitch together multiple tools that struggle to work cohesively," says the CEO.

This challenge was compounded by a third, and more urgent, realisation: AI operates at a speed that no human can realistically triage. Modern attackers are increasingly leveraging AI, generative AI, and large language models to automate attacks. They gain access using valid credentials, then rapidly delete, modify, or exfiltrate production data. Almost simultaneously, often within seconds, they target and delete backups, which are typically an organisation's first line of defence. In such scenarios, human-led response simply cannot keep pace.

For Eswaran, this reinforced two critical truths. First, data security must be addressed end-to-end, with privacy and governance applied consistently across both primary and backup data. Second, only a unified platform, one capable of operating at machine speed, can realistically respond to AI-driven threats.

Initially, Eswaran believed the solution might lie in combining two or three different security technologies alongside Veeam's best-in-class data resilience platform. But as customer conversations evolved, that assumption began to change. Around two to three years ago, following the emergence of the first generative AI models,

Anand Eswaran
CEO
Veeam



customers began voicing a growing sense of frustration. They found themselves acting as the triage point between data security, privacy, compliance, and resilience—managing each domain separately and attempting to stitch them together internally.

This fragmentation, Eswaran believes, explains why so many AI initiatives fail to scale. While industry narratives often point to shortages of GPUs, compute capacity, or immature LLMs, the real issue lies elsewhere. "AI projects struggle because organisations lack the right data security, privacy, and compliance controls for the data feeding their models. And when failures inevitably occur, most organisations lack the ability to return to a known safe state with precision, coordination, and speed," he says.

That realisation triggered a fundamental shift in thinking. The only viable path forward for Veeam, according to the CEO, was a single, unified platform that brings together security, privacy, compliance, governance, and data resilience into one coordinated framework. Done correctly, such a platform does more than protect data; it enables AI to scale safely across the enterprise.

It was within this context that Securiti AI stood out. Among its most defining strengths is its approach to data security itself, a notoriously complex and high-stakes challenge. Central to this approach is the Data Command Graph, a visual representation of an organisation's entire data estate. Often likened to a social network for enterprise data, the graph shows where data resides, who has access to it, and how different data elements relate to one another. It maps which agents interact with which datasets, how data is used across AI model lifecycles—from pre-training to mid-training and post-training—and which models are consuming which information. From an architectural perspective, Eswaran describes this graph-based visualisation as exceptionally difficult to replicate.

Another critical differentiator is Securiti AI's microservices-based product architecture. This design enables the platform to move at extraordinary speed. As new AI innovations emerge, the platform can integrate next-generation models through its connector framework in a matter of weeks rather than years. In an environment where AI innovation cycles are accelerating rapidly, this level of agility is no longer a nice-to-have—it is essential.

Execution, however, is where vision becomes reality. Too often in the security industry, acquisitions are announced and customers wait months or even years to see meaningful product integration. In this case, integration moved at a very different pace. Within days of closing the acquisition, unified capabilities were already being demonstrated to customers and partners. The first generally available products from this unified platform roadmap are expected as early as Q1 of this year.

Ultimately, Eswaran believes that the pace of innovation is one of the clearest indicators of architectural quality. In bringing together Veeam and Securiti AI, the objective is not incremental enhancement, but a fundamental rethinking of how data is secured, governed, and recovered in the age of AI. "When those foundations are in place, organisations don't just protect their data; they unlock the full potential of AI at scale," he concludes.

The age of intelligent security

Axis Communications is redefining what physical security means in an increasingly digital and connected world.

The physical security industry is in the midst of a fundamental transformation. What was once defined by passive surveillance is rapidly evolving into an ecosystem of intelligent, AI-driven, and data-centric systems that actively shape how organisations operate, respond, and make decisions.

At the forefront of this shift is Axis Communications, a market leader that has significantly expanded both the depth and breadth of its portfolio as security converges with intelligence, analytics, and real-time insight.

We recently sat down with Loubna Imenchal, the newly appointed Regional Director of Axis Communications, along with Rudie Opperman, Regional Manager of Engineering and Training, to discuss how the company is redefining its role in a rapidly evolving digital and security landscape.

"Axis is globally known as the inventor of the IP network camera and a pioneer of modern security. That foundation remains core to who we are," says Loubna. "But today, Axis is not defined by a single product category—we are a technology leader delivering open, intelligent security solutions that create long-term value for societies and businesses."

Loubna Imenchal
Regional Director for Middle East, Türkiye, Central Asia and Africa at Axis Communications

> "With the rise of generative AI, we're now moving from insight to autonomy. Systems are beginning to act, not just observe. That shift will define the future of surveillance—and intelligent infrastructure more broadly."

That shift in identity sits at the heart of Axis' current strategy. Today, the company positions itself as an intelligent infrastructure provider, operating at the intersection of AI, IoT, and edge computing, against the backdrop of global digital transformation.

"Security is no longer just about protection—it is about insight," Loubna explains. "Network cameras are among the most powerful and underutilised data sources in organisations today. When that data is responsibly transformed into intelligence and connected across systems, security investments evolve into strategic platforms that drive efficiency, resilience, and smarter decision-making."

This strategic evolution is precisely what attracted her to Axis. She describes the company as a rare combination of category leadership, principled ethics, and deep technological innovation—anchored by a long-term vision rather than short-term cycles.

"As AI, cloud, and analytics reshape our industry, Axis was among the first to recognise that the future would not be built in isolation," she says. "The company made a deliberate choice to invest in an open, ecosystem-driven model—bringing together partners, system integrators, and software innovators. That approach creates sustainable growth and significant expansion opportunities, particularly across the region my team and I lead."

For Loubna, the timing is pivotal. She views the shift toward intelligence-led systems as a once-in-a-generation transformation. "These moments are rare. They redefine industries and how value is created. Being able to lead at the intersection of technology, responsibility, and real-world impact is exactly where I want to be."

That transformation is already evident in

Axis' technology roadmap. The company has evolved well beyond traditional surveillance, toward AI-enabled devices, sensors, and edge intelligence capable of generating real-time, actionable insights. These technologies not only enhance decision-making but significantly reduce false alarms and operational friction.

"With the rise of generative AI, we're now moving from insight to autonomy," Loubna notes. "Systems are beginning to act, not just observe. That shift will define the future of surveillance—and intelligent infrastructure more broadly."

As intelligence and automation accelerate, cybersecurity and trust become non-negotiable. For Loubna, they are foundational, not afterthoughts. "As organisations adopt AI- and cloud-based architectures, trust is the enabler of scale. Leading this transformation means leading responsibly."

In parallel, Axis is expanding across multiple industry verticals, applying its open platforms to smart cities, data centres, retail, critical infrastructure, and workplace safety. The ambition is not to solve isolated us cases, but to build scalable, cross-industry intelligence platforms.

None of this happens in isolation.

"Ecosystems are how innovation scales," she says. "Partners, system integrators, and software developers are central to delivering real-world impact and long-term value."

Looking ahead, Loubna distils Axis' direction into four core pillars: products, platform, value, and trust. "When these come together, intelligent infrastructure moves from promise to reality—and fundamentally changes how organisations operate."

A hybrid blueprint

The tectonic shift toward intelligent security systems naturally raises a critical question: where should that intelligence live? The answer brings architecture and infrastructure into focus, spanning cloud, on-premises environments, and edge computing.

"What's important to emphasise is our philosophy around where technology should reside," says Rudie. "For us, this is not an either-or conversation. We believe in choice, and we aim to give both our customers and partners the flexibility to decide what works best for them. In most cases, a hybrid approach is the right answer, as requirements vary depending on the use case and business priorities."

In surveillance environments, where data must often be acted on in real time, latency becomes a defining factor. When immediate response is critical, edge computing plays a central role. Advanced analytics can take place directly on the camera itself, at the edge, exactly where events are occurring.

At the same time, many organisations are embracing cloud-based models for the scalability they provide, along with the ability to gain centralised visibility across multiple sites. Cloud platforms also simplify system maintenance, firmware updates, and the rollout of new capabilities from a single point of control.

From Axis' perspective, these models are complementary rather than competitive. "The future is not about choosing cloud over edge, or vice versa. It lies in intelligently orchestrating both, ensuring systems work together seamlessly to deliver operational efficiency and real-time insight at scale," says Rudie.

Intelligence in action

To illustrate how intelligent surveillance is delivering real-world impact, Rudie points to one of the most demanding operational environments of all: the modern airport.

"Airports are incredibly complex ecosystems," he says. "You have aviation operations, transport, hospitality, retail, and logistics. It's organised chaos, and every second counts."

That complexity is precisely where intelligent surveillance is beginning to show its value. For airport operators, efficiency and profitability are not abstract goals; they are business imperatives. Delays, bottlenecks, and wasted resources have a direct financial impact in an industry where margins are under constant pressure.

On the airside, AI-enabled surveillance cameras are increasingly being used to support aircraft turnaround management. From the moment an aircraft lands to the moment it departs, cameras track the docking process and each servicing milestone; unloading, refuelling, cleaning, passenger disembarkation and boarding.

Baggage handling presents a similar opportunity. Beyond security, ensuring luggage isn't lost or stolen, intelligent surveillance helps identify bottlenecks, downtime, or system failures along the baggage journey, from aircraft to conveyor belt to reclaim area.

"When something breaks down, it needs to be flagged immediately," Rudie says. "That allows the right people to be deployed quickly and the issue resolved faster."

However, responding to these events at scale requires more than visual insight alone. This is where integrated communication becomes critical. Axis has invested heavily in IP-based audio systems that can automatically respond to AI-detected events based on predefined rules.

Audio announcements can be triggered dynamically based on what the system detects. Recognising that not everyone responds to audio cues, Axis has also introduced intelligent display speakers, combining sound with visual messaging.

On the aviation side, camera intelligence extends even further. Because Axis devices support applications at the edge, partners have developed solutions that support operational visibility around aircraft landings and take-offs using standard PTZ cameras. Integrated with aviation tracking systems, these cameras automatically identify incoming aircraft, zoom in, and record high-resolution footage tagged with time, date, and aircraft number.

The same intelligence-driven approach is now being applied across a growing number of industries, each with its own operational challenges.

"In smart cities, traffic flow is one of the biggest issues we see," says Rudie. "You have large volumes of vehicles moving across highways and intersections, and even a small anomaly can quickly create safety risks or congestion."

Intelligent surveillance systems are increasingly used to detect these anomalies in real time. A vehicle stopping unexpectedly on a highway, for example, can be automatically identified, flagged, and responded to, often before the situation escalates.

Retail environments present a different set of priorities. "In retail, it's all about customer behaviour," Rudie explains. "It's about understanding flow, optimising conversion, and responding quickly when things like queues start to build up."

Surveillance systems monitor footfall patterns and queue lengths, enabling retailers to adjust staffing levels dynamically. As in airports, communication can be delivered audibly, visually, or through

Rudie Opperman
Regional Manager of
Engineering and Training
Axis Communications

on-screen text, helping guide customers and improve overall experience.

Critical infrastructure, particularly data centres, brings yet another set of demands. "In data centres, it's all about uptime," Rudie notes. "Everything has to work as close to continuously as possible."

Intelligent surveillance systems provide situational awareness across multiple layers of these facilities, monitoring processes, detecting incidents early, and enabling rapid or automated responses to ensure infrastructure operates exactly as designed.

Across all these use cases, the technology remains fundamentally the same. "It's the same platform and the same intelligence," Rudie says. "What changes is how it's applied."

Loubna believes this is where surveillance is headed, and where Axis is focusing its efforts. "We spend a lot of time educating the market. That means working closely with partners and asking everyone to think beyond the camera and focus on real business impact."

For Axis, innovation is no longer about adding features. It's about helping organisations operate better, regardless of industry. That shift, she stresses, depends on a strong ecosystem.

"We can't do this alone. Faster innovation only happens when partners are aligned with the vision."

Long-term flexibility is central to that vision. As intelligent systems scale, early technology choices become critical. "If a system can't coexist with others or lacks security by design, it becomes very costly to replace later," she warns.

That also makes cybersecurity non-negotiable. At Axis, it is engineered into the product from the outset, spanning hardware, firmware, and the broader supply chain. "Security isn't an add-on," Loubna says. "It's built in from day one."

Secure hardware, encrypted key storage, and continuous lifecycle management ensure systems remain protected as they evolve. This allows customers to innovate and integrate with confidence.

"Openness only works when trust is engineered in," Loubna adds. "You need systems that connect, but you also need accountability."

Axis' role, she concludes, is clear: turning real-world activity into actionable insights, delivered with security and scale built in.

"With Intersec approaching, that's the message we want to leave with the market," Loubna says. "Innovation matters. But trust matters just as much."

Bridging the **divide**

Raja Patel, Chief Product Officer at Sophos, on why breaking down silos to key to optimising cyber insurance investments.

In a cybersecurity landscape populated with increasingly complex threats, an integrated approach to cyber risk management that balances security controls and cyber insurance is crucial. But many organizations still operate in silos when purchasing a cyber insurance policy. For example, IT teams that build and maintain cyber defenses may supply security control information for insurance applications—but have little input into policy scope and coverage levels.

That's a missed opportunity. Organizations that coordinate their cybersecurity protections with their cyber insurance efforts can improve both their defenses and insurance positions, lowering costs and enhancing protection at the same time.

But this requires participation and collaboration from leaders across different business units. It's up to business and IT leaders to facilitate more effective collaboration so their teams can optimize cyber insurance investments.

Consequences Of Siloed Cyber Risk Management

Picture this: Your IT team implemented advanced security measures and conducts routine vulnerability assessments to ensure your organization's digital assets are protected. However, your procurement team that manages the organization's insurance policies is unaware of the IT team's security efforts. When it comes time to negotiate coverage options for cyber insurance, procurement misses opportunities for premium reductions and more favorable insurance terms based on existing protections.

This scenario illustrates just one way that siloed planning can hinder an organization's cyber insurance position. A lack of collaboration throughout the process can also cause an organization to underestimate the amount of coverage it needs or prioritize the wrong aspects of an insurance policy.

Moreover, siloed planning can lead to confusion about what an organization's insurance actually covers—which is more common than you might expect. Among organizations with a cyber insurance policy, 43% of cybersecurity and IT leaders think their policy covers breach notification support but aren't certain. These oversights can undermine the value of your cyber insurance investment, often resulting in higher premiums, inadequate coverage, insufficient support and hindered recovery in the event of a cyberattack.

Considerations For Effective Cyber Insurance Planning

A unified and holistic approach to cyber risk planning can significantly improve your insurance position and defenses. If you've managed cyber risk the same way for years, it's time to elevate your strategy. By prioritizing cross-functional collaboration and proactive planning, you can secure optimal insurance coverage and better

Raja Patel
Chief Product Officer
Sophos

protect your assets.

1. Start early.

Don't wait until your cyber insurance renewal is approaching to start planning. Being proactive allows you to shop for insurance providers, negotiate better terms, gather requirements and implement or improve controls. It also enables strategic investment planning.

For example, let's say your IT team wants to adopt a managed detection and response (MDR) service, but your finance team tells them there's no budget for it. After evaluating the situation more closely, the teams discovered that investing in MDR would significantly improve the organization's cyber insurance position, unlocking cost savings on premiums they can reallocate to fund the service.

Allowing adequate time for researching and comparing insurance providers and policies results in more informed decisions and helps you avoid rushed choices that leave gaps in coverage.

2. Establish internal alignment.

Starting the cyber insurance process early also ensures there's time for stakeholders to align internally before taking action. Start by identifying who should be involved—typically, leaders from IT and cybersecurity, finance, procurement, legal and compliance.

Once you've designated your key stakeholders, consider holding a kickoff meeting and establishing a channel for ongoing communication. During this initial phase, take stock of your current cybersecurity measures and any gaps in insurance coverage. Make sure you also clearly define stakeholders' roles and responsibilities to ensure accountability and alignment between your cyber insurance strategy and overarching business objectives.

3. Consider your unique needs.

Proactive planning allows you to conduct a comprehensive evaluation of your organization's specific risk profile and insurance needs. Stakeholders from different business units have unique perspectives and drivers for coverage, so it's smart to create a document that serves as a single source of truth regarding coverage needs.

As you document your insurance needs, make sure to address coverage scope, policy limits and deductibles. It's also important to maintain consistent communication between cross-functional stakeholders and the team actually managing your insurance application (likely from procurement). Your investments will only be recognized by insurers if the quality of your defenses is understood and clearly conveyed in the application.

Level Up Your Cyber Resilience With Holistic Planning

Before applying for cyber insurance, have you taken time to evaluate your cybersecurity posture, assess your risk profile and achieve internal alignment among key stakeholders? If you haven't, it's not too late to adopt a more integrated and cross-functional approach to your cyber insurance strategy.

Cyberattacks impact nearly every aspect of a business, from financial stability to operational continuity. That's why leaders from across the organization must work together to coordinate their cyber defenses and insurance. With stakeholders working together, you can make smarter cybersecurity and cyber insurance investments, leading to reduced risk and lower costs—bolstering your resilience in the face of modern cyber threats.

The cyber reckoning

Inside the security landscape of 2026

Andrea Multari
Vice President of Cyber Defense
CPX

Ezzeldin Hussein
Regional Senior Director, Solution Engineering – META,
SentinelOne

Looking ahead to 2026, cybersecurity leaders are largely aligned on one point: the nature of threat has fundamentally changed. The coming year will be defined by identity-centric attacks, machine-speed automation, and growing pressure on critical infrastructure, forcing enterprises to rethink both defence and resilience.

Andrea Multari, VP- Cyber Defense at CPX, describes the MENA region as standing at a strategic inflection point, where identity has become the new frontline. Attackers, he notes, are no longer focused on breaking through perimeter defences. Instead, they are logging in using stolen credentials, often blending seamlessly into legitimate activity. Ransomware has also evolved, shifting away from pure data encryption toward operational disruption, with attackers deliberately targeting sectors that cannot afford downtime.

At the same time, operational technology has undergone significant change, expanding the attack surface and exposing new vulnerabilities as connectivity deepens across industrial environments.

That shift toward identity-driven attacks is echoed by Harish Chib, Vice President Emerging Markets, Middle East & Africa, Sophos, who expects 2026 to mark a move away from broad, opportunistic ransomware campaigns toward AI-powered, highly targeted operations. Deepfake voice fraud, agentic-AI-driven CEO impersonation, large-scale crypto theft, and AI-augmented insider risk are all expected to rise. Threat actors, ranging from sophisticated Western ransomware groups to state-linked operators, will increasingly weaponise automation, social engineering, and supply-chain infiltration.

For organisations, this means preparing for faster, more convincing attacks, alongside tighter regulatory scrutiny and growing demands for managed detection and response, identity protection, and security awareness.

Mohammed Aboul-Magd, VP of Product, Cybersecurity Group, SandboxAQ, frames the challenge as a machine-speed crisis. By 2026, he argues, the rapid proliferation of non-human identities—API keys, service accounts, certificates, and autonomous agents—will create a vast and poorly governed attack surface. In many cases, attackers will not exploit software flaws at all; they will simply log in using exposed machine credentials buried deep within shadow infrastructure.

Jozsef Gegny, Senior Security Researcher at Acronis TRU, places these trends within a broader geopolitical context. He sees cybersecurity increasingly shaped by autonomy, identity-focused defences, and the fragmentation of the internet driven by data sovereignty laws. AI-accelerated attacks will become the norm, with adversaries automating reconnaissance, exploit selection, social engineering, and lateral movement. At the same time, supply-chain risks will intensify, as attackers target open-source ecosystems, managed service providers, and even AI model supply chains to trigger cascading failures across organisations.

For Hussam Sidani, Vice President for the Middle East and North Africa at OPSWAT, the most concerning development is the growing focus on critical infrastructure. Cybercriminals are becoming more strategic, increasingly targeting sectors such as healthcare, water services, and regional

Harish Chib
VP Emerging Markets – Middle East and Africa, Sophos

Hussam Sidani
Vice President - Middle East and North Africa OPSWAT

James Maude
Field CTO
BeyondTrust

energy providers—organisations operating on tight margins, long funding cycles, and ageing infrastructure. Their inability to modernise operational technology and cybersecurity simultaneously makes them high-impact, high-leverage targets.

Mohammed AlMoneer, Senior Director, Turkey, France, Africa and Middle East at Infoblox, adds that by 2026, cybersecurity will be shaped by AI-driven automation, hyper-distributed infrastructure, and persistent identity abuse. Attackers will deploy more automated, highly personalised campaigns that continuously probe hybrid and multi-cloud environments. Domain abuse, DNS tunnelling, and short-lived malicious infrastructure designed to evade traditional tools will become more prevalent.

In response, he argues, organisations must move beyond reactive detection toward preemptive control, particularly at foundational layers such as DNS and core network services—turning what was once considered digital "plumbing" into a strategic security asset.

Agents of change

The rise of agentic AI is set to fundamentally reshape both cyberattacks and cyberdefence in 2026, accelerating the shift toward automation on both sides of the security equation.

Ezzeldin Hussein, Regional Senior Director, Solution Engineering, SentinelOne, expects adversaries to increasingly deploy autonomous attack elements capable of conducting reconnaissance, exploiting identity gaps, adapting in real time, and moving laterally without human oversight. These AI-driven attacks will be faster, more precise, and far more difficult to detect using traditional, signature-based security tools. Static defences, he warns, will struggle to keep pace with threats that can continuously learn and adjust their behaviour mid-attack.

On the defensive side, however, the same technology will drive a parallel transformation. Enterprises will begin adopting AI-native, autonomous security operations, with security operations centres evolving toward self-directed models. Agentic AI will correlate signals across endpoints, cloud workloads, identity systems, and networks, enabling containment and recovery to occur at machine speed. The result, Ezzeldin notes, will be a dramatic reduction in dwell time and operational burden for security teams.

James Maude, Field CTO at BeyondTrust, highlights another critical dimension of this shift: the rapid proliferation of non-human identities. As organisations race to adopt AI tools—often without formal governance—the number of API keys, service accounts, certificates, and agent credentials is growing exponentially, far outpacing human identities. Many organisations, he says, have already lost visibility and control over this expanding attack surface. Compounding the issue, AI introduces new classes of vulnerabilities that do not fit neatly into traditional threat models, further increasing complexity for defenders.

For Andrea, agentic AI represents not just a defensive capability, but the future foundation of cyber resilience. He sees autonomous security playing a critical role in embedding security by design earlier in the software development lifecycle, ensuring systems are secure by default rather than patched after deployment. As data increasingly becomes a strategic national asset, these AI-driven defences will be essential to protecting sovereignty and ensuring critical infrastructure operates with confidence and continuity.

Data sovereignty reshapes the cloud security playbook

As data sovereignty laws multiply across regions, cloud security strategies are being forced into a fundamental rethink. By 2026, security architectures will no longer be designed around a single global control model, but around a balance between global consistency and local enforcement.

Mohammed from Infoblox believes data sovereignty will push cloud security to become both global and local at the same

Jozsef Gegeny
Senior Researcher
Acronis TRU

Mohammed Aboul-Magd
VP of Product, Cybersecurity Group
SandboxAQ

Mohammed AlMoneer
Senior Director, Turkey, France, Africa and Middle East
Infoblox

time. Organisations will need to apply consistent policies and threat detection across their environments while respecting country-specific rules on data residency, processing, and access. This shift will drive the rise of regionalised control planes and in-region enforcement models, where sensitive telemetry—such as DNS and identity data—is analysed and acted on close to where it is generated, rather than being funnelled back to a central stack. For CISOs, sovereignty will no longer be a late-stage legal consideration; it becomes a core design principle embedded into cloud, network, and security architecture from day one.

Harish from Sophos sees a similar trajectory, with cloud strategies evolving toward regionalised data processing, tighter identity controls, and sovereignty-aware architectures. As organisations gain clearer visibility into where data resides, who accesses it, and how AI systems interact with sensitive information, adoption of cloud-native security controls will accelerate. Encrypted AI workflows, regionally aligned MDR services, and locally operated SOCs will become essential to meeting regulatory demands without sacrificing operational agility.

Together, these shifts point to a future where cloud security is no longer about scale alone, but about control, visibility, and trust across jurisdictions.

Proving cyber ROI when budgets tighten

With security budgets under pressure, CISOs are being challenged to demonstrate tangible returns on investment while still strengthening resilience. The conversation, many argue, must move away from fear-based narratives and toward measurable business impact.

Mohammed from SandboxAQ suggests reframing cybersecurity around friction reduction. Manual identity and certificate management slows development, causes outages, and creates operational fire drills, with certificate expirations already a leading cause of downtime. Automating cryptographic and identity lifecycles eliminates these disruptions, frees engineering capacity, and delivers immediate operational ROI.

Andrea agrees that CISOs must evolve from technical gatekeepers into strategic business enablers. Securing executive support means translating cyber risk into business language and focusing on measurable risk reduction rather than accumulating tools. Automation in areas such as identity and access management or password self-service not only improves security posture, but also reduces costs and enhances user experience. By aligning investments with enterprise KPIs and prioritising modular, risk-based solutions, cybersecurity becomes a driver of continuity and growth rather than a cost centre.

Ezzeldin reinforces this view, arguing that ROI must be tied directly to resilience. As budgets shrink, priorities should centre on operational efficiency, risk reduction per dollar spent, and platform consolidation. AI-driven automation that lowers detection and response times, reduces analyst workload, and prevents incidents from escalating delivers measurable financial value. Metrics such as downtime avoidance, identity risk reduction, and exposure management resonate far more clearly with boards than abstract threat statistics.

James adds a practical reality check: security is notoriously difficult to measure because it is often about preventing events that never occur. One effective approach is to focus on visibility of the attack surface and track its reduction over time. In identity security, understanding which identities have paths to privilege—and which carry the largest blast radius if compromised—allows organisations to prioritise resources where they matter most and clearly demonstrate risk reduction.

The message for CISOs is increasingly clear. In an era of constrained budgets, the strongest case for investment is showing how security keeps the business running, reduces friction, and enables resilience at scale.

Path to sustainable **digital defence**

Noman Qureshi, Cyber Security Lead dnata UK (The Emirates Group) writes about the intersections of cybersecurity and AI with carbon emissions.

In today's ultra connected world, Artificial Intelligence (AI) and cybersecurity have become foundation of digital resilience. AI-powered threat detection, prophetic analytics, and automated response centres are transforming how organizations defend against cyberattacks. Though, this high-tech progress comes with an environmental cost due to growing carbon footprint. As organizations scale the digital defences, the consumption of energy for AI models and cybersecurity infrastructures is surging, raising significant questions about sustainability. This article throws spotlight on the correlation of cybersecurity & AI with carbon emissions, referred by few statistics and proposed strategies for greener digital defence.

Organization's digital transformation strategy mainly contain the huge adoption of AI powered Tools and Technique which is unquestionably a much needed strategy in this highly competitive environment, in fact huge companies would keep making AI driven approach as part of their DNA but they are also realizing that this fast moving change precisely pertaining to AI & cybersecurity systems are among the highest energy components as to train large AI models and operating real-time threat monitoring tools require enormous computational power that resulted into significant carbon emissions.

According to a recent UN report, AI-related activities generated 80 million tonnes of CO2 emissions in 2025, and this is almost equivalent to the annual emissions of mega cities. An advanced language model's training may use as the same amount of energy as 130 American households for a year, while inference tasks i.e. to train and to make predictions or analyse new data add constant demand. Furthermore, 765 billion Liters of water were used in 2025 to cool AI data centres, exceeding the amount of bottled water used worldwide.

Energy consumption has significantly increased due to the exponential growth of cybersecurity operations, which standout an increase of 30% in worldwide defences in Q2 2024. As per studies, data centres use 240–340 terawatt-hours per annum, or 1% to 1.3% of the world's total electricity consumption which resulted the emissions from data centre 105 million metric tons of CO2 in 2024, a frightening 300% jump since 2018. By 2030, projected consumption that emissions may exceed 2.5 billion metric tons. likewise, the most prominent platforms for Security Information and Event Management (SIEM) are exceptionally carbon rich as, according to studies, operational energy consumption accounts for 75% of SIEM expenditures because these systems analyse logs 24/7 to monitor irregularities.

Organizations would be playing key role by putting pressure on power infrastructures consumption if current trends continue and they would also be

Noman Qureshi
Cyber Security Lead
dnata UK (The Emirates Group)

threatening international sustainability objective by 2030 as AI workloads and cybersecurity operations may encounter up to 20% of the global electricity.

This is pertinent to mention, if organizations implement environmentally responsible practices that lower emissions without sacrificing protection to balance security and sustainability then digital defence's effects on the environment are no longer a specialized issue. This objective can be accomplished by optimizing algorithms and employing lightweight models for effective anomaly identification. Consumption of Energy can be substantially reduced through the implementation of established best practices, wherein enhanced RFM - Random Forest models that sustain high levels of detection accuracy. These enhanced Random Forest models provide a range of benefits that render them highly valuable in practical implementations which includes but not limited to spotting patterns and making accurate predictions, reduce rate of errors while identifying cyber threats or classifying data. In addition, these models are also more competent by delivering quicker results during crucial real-time scenarios like securing a cyberattack as it unfolds. Therefore, by optimizing and implementing Random Forest models organizations can ingesting less computer power, that ultimately save electricity, reduces costs, and results in better for the environment. These models even have capability of handling larger and more complex datasets without slowing down or crashing, and they are designed to avoid overfitting by learning the model of training data including all the small details and even the random noise rather than just the underlying patterns. As a result, the model performs efficiently and effective on the data as it was trained, and they also perform reliably even with new data. Moreover, these streamlined models are simpler to set up and cheap to maintain, as they require less fine-tuning, and they can be customized to focus on customized needs, such as targeting certain types of threats or operating within strict energy limits.

In summary, enhanced Random Forest models are smarter, and more efficient, serving organizations to make better decisions by saving less energy, and adapt to changing demands making them a valuable tool in fields like cyber security and consume 40% less energy than XGBoost.

Another effective approach of lowering emissions can be switching to carbon-neutral cloud platforms and work together with suppliers who utilizes cutting-edge cooling systems and renewable energy. Hardware consolidation and virtualization further cut down on unnecessary energy use.

Above all improved and enhanced methods should be driven via establish governance structures that monitor emissions from workloads involving AI as trends are showing red flag picture which is also reported by tech giants: Microsoft's Scope 3 emissions increased by 30.9% in 2023, while Google's emissions increased by 48% since 2019, primarily as a result of generative AI adoption. [

Industry should also collaborate on a single forum to develop Industry-wide guidelines that combine environmental goals with cybersecurity are critical. Complying with ESG guidelines guarantees regulatory compliance and satisfies investor expectations.

Technological advancement would continue to grow, and world would continue to see the massive use of AI, simultaneously AI security via cyber security control would also keep increasing and evolving as per country and as per organization's Threat Landscape, so, two challenges i.e. safeguarding our data and protecting the environment should be strategically handled together which will help us to create a safe digital future that supports global climate goals by integrating sustainability into cybersecurity and AI practices, from energy-efficient algorithms to green infrastructure. Thus, Green digital defence is urgently needed.

Tracking the **adversary**

Ahmad Halabi, Managing Director of Resecurity, outlines the cybersecurity vendor's plan to to ramp up its presence in Saudi Arabia and support the Kingdom in strengthening its defenses against evolving cyber threats.

At Black Hat last year, you have made some major announcements and investments as part of your expansion in Saudi Arabia. Can you take us through that?

Yes, we've been heavily investing in Saudi Arabia and working closely with the government, as well as with the US–Saudi Business Council. Our goal is to ensure we deliver the strongest possible cybersecurity capabilities to the country and support national efforts to defend against all types of cyber threats. Saudi Arabia is a very important market for us. We are committed to serving it as extensively as possible, and we believe we're doing meaningful work there. We're happy to support in any way we can.

Are you setting up a local SOC or making other specific investments in the Saudi market?

Our focus in Saudi Arabia is on delivering Cyber Threat Intelligence products and services. This includes everything related to protecting customer brands across the internet, such as monitoring for data breaches, dark web activity, social media threats, impersonation attempts, and intellectual property infringement.

We continuously monitor the broader internet ecosystem to identify any potential threats targeting our customers. This allows us to alert them early, often before an incident escalates, so they can take swift action to prevent business disruption, reputational damage, or financial loss.

Do you localise your research?

Yes, absolutely. We have a local team on the ground and make significant investments in talent development. We actively support Saudi graduates by signing MOUs with universities, providing free training programs, and offering internship opportunities. Building local capability is a key priority for us.

You have built a strong reputation in cyber threat intelligence. How do you differentiate yourselves from other vendors?

There are several factors. First is local presence and responsiveness. Because we have a localised team, we can respond extremely quickly, often within an hour. We stay very close to our customers during incidents and act as an extension of their internal teams whenever support is needed.

Second is the quality of our intelligence. We invest heavily in research and development, investigations, and proactive threat hunting. We focus on building detailed threat intelligence and asset mapping within the country, not just monitoring threats originating outside the region.

To support this, we have dedicated local capabilities, including a Counter Fraud Unit and a Threat Intelligence Unit operating within the country. This allows us to maintain deep visibility into the local threat landscape and deliver intelligence that is both timely and highly relevant.

Ahmad Halabi
Managing Director
Resecurity

Can you tell us how your platform collects, correlates, and operationalises threat intelligence?

We operate a core Fusion Center where all threat intelligence data is centralised. This data is distributed across thousands of servers to ensure resilience and avoid any service interruption, which is why the platform runs 24/7 without disruption.

We continuously monitor a wide range of sources across the open web, social media, deep web, dark web, Tor networks, and other online ecosystems. In addition, we onboard dozens—and sometimes hundreds—of new data sources every day. If a customer is mentioned, or if there is any indication of a potential breach or incident related to them, we notify the customer immediately.

How do you turn all of that data into actionable intelligence and insights for clients?

We do this through threat risk prioritisation and scoring. We assess whether a customer is genuinely being targeted and whether there is a material breach—yes or no. If the answer is yes, we assign a higher risk score, take immediate action, and report it to the customer right away. This ensures that customers focus only on threats that truly matter.

When it comes to the threat landscape, are you seeing an increase in AI-driven exploits?

Yes, absolutely. We are seeing more incidents driven by automation and AI, as attackers are increasingly using these technologies to scale and accelerate their attacks. In response, we are also developing AI-based capabilities for defensive and security purposes.

At the same time, we actively track threat actors who use AI. While they may leverage automation, they also leave patterns, mistakes, and behavioral signals. These indicators allow us to identify and track them over time.

What are your plans for the rest of the Middle East? Are you planning to expand further in the region?

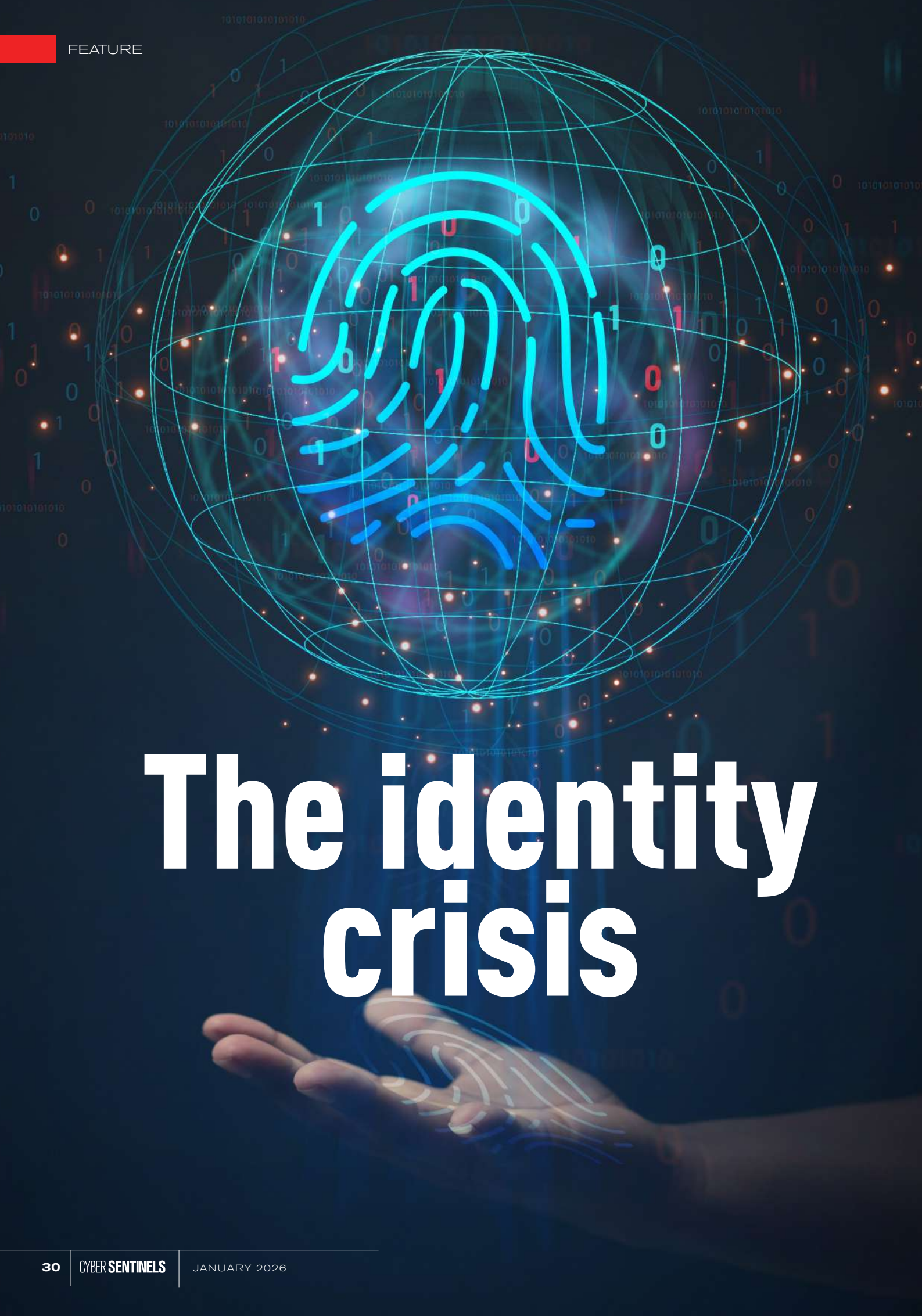
We are already present across the GCC, as well as in the Middle East, Africa, Europe, and Asia. We are deeply involved in threat monitoring, detection, and response across these regions.

We maintain a strong base of localised and regional support teams to ensure comprehensive coverage. This is important because many incidents that impact Saudi Arabia or the GCC do not necessarily originate there. By monitoring neighboring regions and global threat activity, we can identify and respond to threats that may be launched from outside the local environment.

Given the geopolitical environment, are you seeing an increase in nation-state attacks in the region?

Nation-state attacks are not going to stop. The key challenge is not always identifying exactly who is behind an attack, which can be extremely difficult, but understanding the intent and potential impact of the attack.

What matters most is ensuring that security controls are properly deployed and that organisations have robust threat intelligence and monitoring systems in place. These systems must be capable of alerting organisations to all types of threats, whether they are nation-state advanced persistent threats or financially motivated actors attempting to steal money or data.



The identity crisis

With the alarming surge in identity-based attacks, identity and access management has become a top priority for CISOs.

Identity has quietly become one of the most strategic assets in the digital enterprise. What was once treated as a security control function is now central to how organizations operate, innovate, and build trust at scale.

As AI-driven systems make autonomous decisions, cloud-native platforms dissolve traditional boundaries, and regulators demand greater accountability, identity is emerging as the connective tissue that holds it all together. In this new environment, how identities are created, governed, and trusted is no longer a technical detail - it is a defining business imperative.

Though the concept of identity as the new perimeter is not new, industry pundits say 2026 is the year it becomes operational reality.

According to Laurence Elbana, Director, Sales – Middle East, CyberArk, the rapid rise of cloud and hybrid environments—combined with work-from-anywhere operating models—has fundamentally blurred the boundaries of the traditional, network-centric security perimeter. In a world where users, applications, and data are distributed across multiple platforms and accessed from countless devices, perimeter-based defenses can no longer reliably protect critical assets.

In this new reality, identity, whether human or machine, has become the primary battleground. Identity security is now essential because it represents the only control plane capable of consistently enforcing verification and least-privilege access across every critical system. As the attack surface continues to expand, identity-based controls play a decisive role in defending organizations against modern threats, including ransomware, credential abuse, and insider risk.

Morey Haber, Chief Security Advisor at BeyondTrust, notes that in today's cybersecurity climate, it is often easier for attackers to log in than to hack in. Traditional vulnerabilities and exploits have a limited lifespan, typically closing once patches are applied, while zero-day attacks are expensive and complex to develop. By contrast, stealing credentials and secrets offers a far more efficient and reliable path into an organization.

Why would threat actors invest significant time and resources attempting to breach systems through exploits, Morey asks, when valid login credentials can provide access that appears legitimate, blends into normal user behavior, and often persists long after software vulnerabilities have been remediated? This shift does not mean exploits have disappeared, but it does signal that they are no longer the primary method used to compromise organizations.

According to Jay Reddy, Head of Growth at ManageEngine, the enterprise network perimeter once defined the core security boundary, with implicit trust granted to users and devices operating inside it. Over the past decade, however, that traditional perimeter has quietly—and decisively—disappeared.

As workloads have shifted to the cloud, employee identities now span dozens of applications and services. In this distributed environment, attackers no longer need to break through defenses; they simply log in. Identity has therefore emerged as both the central control plane and the primary detection surface across users, applications, and systems.

For security teams, this shift has been transformative. The focus is no longer on protecting the network itself, but on securing identities—both human users and non-human identities (NHIs).

Hybrid cloud and AI: Changing the nature of identity challenges

While human access remains a concern, these ecosystems have led to a rapid proliferation of machine identities such as service accounts, API keys, and container secrets, each of which can operate autonomously and at massive velocity. Machine identities now outnumber humans by 82 to 1 according to CyberArk's 2025 Identity Security Landscape report.

Laurence says this is a significant issue in the UAE, where 92% of organizations define 'privileged user' as applying solely to human identities, yet 42% of machine identities have privileged or sensitive access. Meanwhile, 54% of UAE organizations have experienced at least two successful identity-centric breaches in the past 12 months, according to the report.

Managing access for non-human identities is fast becoming a priority for organizations which must move beyond basic IAM to a comprehensive identity security approach that includes the enforcement of unified policies, and provides dynamic, just-in-time access for human users and machine identities. As the same time, organizations must secure the type of privileged credentials that increasingly underpin the digital infrastructure.

Morey agrees that organizations are forced to rethink about IAM due to the expansion of both human and nonhuman identities and associated accounts. This is fueling the way identities are managed, since many of the accounts are ephemeral, highly privileged, and have access to a wide variety of sensitive information that

Jay Reddy
Head of Growth
ManageEngine

Laurence Elbana
Director of Sales
CyberArk

Morey Haber
Chief Security Advisor
BeyondTrust

may be hosted outside of the organization, and in some cases, outside of your own geolocation.

"Therefore, organizations are rethinking their identity provider strategy, impacts to joiner, mover, and leaver processes from a dynamic perspective, and how paths to privileged access can be exploited," he says.

Jay offers another perspective on how the identity landscape is undergoing a profound transformation, resulting in what he terms "quantum identity states", where a single digital identity now exists simultaneously across multiple operating planes, such as hybrid cloud platforms, IoT infrastructures, and AI-driven systems.

This level of distribution forces organizations to rethink IAM as a real-time control plane that delivers security decisions that are contextual and dynamic.

This shift, Jay notes, is also driving the emergence of adjacent identity management disciplines with a security focus such as identity security posture management (ISPM) and identity threat detection and response (ITDR). These strategies have become essential extensions of IAM in this evolved landscape.

Managing machine identities alongside human users

CISOs face a significant challenge in attempting to gain visibility and control over a rapidly expanding population of machine identities. The CyberArk report reveals that 68% of organizations do not have security controls in place for AI and large language models (LLMs), yet 82% know their company's use of AI creates sensitive access risks. This disconnect is a concern because AI agents rely on credentials such as certificates, API tokens and secrets.

Laurence emphasises that to help secure AI agents as privileged identities, organizations must evolve their identity security strategies and treat AI agents as part of the privileged ecosystem. This does not entail reinventing the wheel, as organizations can expand their existing toolkit to cover a new set of challenges. Key steps to achieve this include applying privileged access management (PAM) to AI agents, extending secrets management and certificate lifecycle automation to all agentic AI workflows, embracing identity convergence, and extend endpoint privilege management (EPM) where needed.

In Morey's opinion, the biggest challenge CISOs face in managing machine identities is ownership. Who owns the identity, is responsible for its lifecycle and maintenance, and how to escalate issues if the identity is in distress. This includes escalations due to a potential indicator of compromise and linkage to activity based on activity logging.

"Establishing ownership for all machine identities is a difficult task for not only new identities used with AI and the cloud, but also all the legacy technology that has already been deployed from service accounts through to API keys. The scope is vast and truthfully one strategy does not work for everyone and everything," he says.

Jay concludes by pointing out that the gap between human and machine identities has expanded significantly. In most enterprises, machine identities now operate at a scale and velocity that far exceeds human users. Yet, their governance frameworks remain fragmented or, in some environments, largely absent.

This compels CISOs to look beyond traditional security checklists while evaluating IAM solutions that govern machine identities. Without unified oversight, machine identities introduce unmanaged trust relationships and high-privilege pathways that an attacker can exploit.

"As a result," Jay explains, "CISOs have to incorporate the concept of an identity fabric as a strategic framework, one that explicitly includes machine identities to strengthen and reshape digital trust across the enterprise."

GEC Global Enterprise Connect

GEC NEWSWIRE

STAY AHEAD
STAY INFORMED
STAY CONNECTED

Stay ahead with **GEC NEWSWIRE** - your instant gateway to everything Tech, Channel, Cybersecurity, Business, AI, and beyond.

From breaking updates and exclusive interviews to videos, insights, and event highlights, GEC NewsWire brings you the pulse of the enterprise world - as it happens.

Fast. Trusted. Insightful.

Because the world of innovation never stands still - and neither do we.

SCAN TO VISIT OUR WEBSITE

Follow the **GEC NEWSWIRE today!**

Get smarter updates, faster.

The new trust **crisis**

Dr Fadi Alhaddadin, Assistant Professor at Heriot-Watt University, explores how AI could fuel a major trust crisis by 2026 through deepfakes, AI-enabled fraud and the erosion of authenticity online.

By 2026, the world may face a trust crisis unlike any before in the digital age. Generative AI, while driving creativity and automation, is eroding the signals we rely on to determine what is real. Deepfakes, AI-enabled fraud, and synthetic identities are undermining verification across governments, financial systems, and online platforms. Without new verification stacks, provenance systems, and identity-assurance frameworks, credibility itself could become scarce.

A Threat Landscape Defined by Scale and Believability

AI-generated content has advanced with remarkable speed, moving from simple face-swaps to hyper-realistic synthetic videos, cloned voices, and fully fabricated personas. Security reports show a surge in AI-driven impersonation attacks, including executive voice-cloning attempts that nearly triggered multimillion-dollar transfers. Fraudsters now use AI to automate social-engineering scripts, mimic accents, generate personal details, and sustain convincing conversations with little to no human effort. Law-enforcement agencies such as Europol warn that AI has drastically lowered the cost and skill needed for cybercrime. Instead of requiring technical expertise or insider access, criminals can rely on AI to produce persuasive audio, video and written content that appears legitimate. This creates a threat landscape where scale and realism amplify each other, enabling thousands of highly tailored phishing messages and deepfake impersonations at minimal time and cost.

Why Traditional Verification Methods Are Failing

Most digital verification methods were built for a time when falsifying media required specialist skills. Today, convincing deepfakes can be created in minutes with widely available tools. Traditional methods like selfie videos, email confirmations and basic liveness checks are increasingly vulnerable as AI can generate synthetic identity videos, mimic blinking and adjust lighting to fool automated systems. Biometrics are also under pressure: voice authentication is weakened by cloning, and facial recognition struggles to distinguish real faces from high-resolution synthetic ones. Social verification is collapsing as videos, photos, audio messages and live calls can now be fabricated with near-perfect realism. Even the "verified badge" model is unreliable, since attackers can build synthetic personas with realistic histories, aged social-media profiles and AI-driven behaviour patterns. The threat is no longer simple spoofing; it is the creation of entirely credible identities.

Verifiability as a Systems Problem

The coming trust crisis is not simply a media problem. It is a systemic issue demanding

Dr Fadi Alhaddadin
Assistant Professor
Heriot-Watt University

multilayered solutions. Businesses and governments must shift from relying on single-point signals to building robust ecosystems of attestation, provenance, and identity assurance.

1. Verification Stacks

A verification stack is a multi-signal, risk-adaptive approach that validates identity and intent across several dimensions. Instead of relying on a selfie or password alone, a modern verification stack may incorporate device and browser fingerprints, network telemetry, behavioural patterns such as typing, navigation and response timing, cryptographic keys, and contextual risk scoring. This makes impersonation significantly more expensive. As the US National Institute of Standards and Technology (NIST) emphasises in its updated digital identity guidelines, strong identity assurance relies on layered, risk-based controls rather than rigid, one-size-fits-all verification steps.

2. Provenance Layers

Provenance layers help mitigate synthetic media by embedding verifiable metadata into digital content, detailing who created it, what tools or edits were used, and when and where it was produced. Standards like C2PA add signed credentials to images, videos and audio files, while W3C PROV provides a shared model for tracking a digital asset's lifecycle. When broadly adopted, these layers form an authenticity trail that is difficult to tamper with. Identity assurance frameworks go further by combining strong identity proofing via documents, biometrics and authoritative records with continuous authentication and cross-platform federated credentials. NIST's updated SP 800-63-4 guidelines emphasise cryptographic attestations, privacy-preserving identity claims and high-assurance federation which are crucial as synthetic identities increasingly threaten financial, government and corporate systems.

Policy and Platform Responsibility

While technology must drive the solution, policy and platform governance are just as important. Governments are drafting laws to regulate harmful synthetic media and assign clearer liability, and social platforms have begun labelling AI-generated content and requiring provenance metadata for sensitive material. But regulation cannot keep pace with rapid model development. Businesses should enforce minimum provenance requirements for high-risk interactions such as financial requests, contract approvals or identity verification and treat unsigned digital assets as untrusted. Industry-wide cooperation, like threat-intelligence sharing, will be essential for detecting emerging deepfake and fraud campaigns.

Rebuilding Trust Before It Breaks

The indicators of a 2026 trust crisis are already visible. Deepfakes and AI-generated fraud are rising faster than defensive technologies, eroding confidence in what we see, hear and receive. But the crisis is not inevitable. By embracing verification stacks, provenance layers and identity assurance frameworks, businesses can reconstruct the signals that underpin digital trust.

Authenticity must become a first-class citizen in digital systems. Without it, the fabric of verification and the transactions that rely on it will surely continue to fray. The time to act is now.

AI at the front **line**

Dubai-headquartered Secure.com has launched a new product, Digital Security Teammate (DST), a category of AI-native security agents built to help security teams. Uzair Gadit, CEO of Secure.com, explains why this launch marks a milestone in the region's push to lead the next wave of AI-driven cybersecurity.

Uzair Gadit
CEO
Secure.com

What problem in the cybersecurity landscape convinced you that the industry needed a completely new product like Digital Security Teammate?

We were drowning in our own alerts. The problem isn't that we lack tools; it's that we have too many of them, all screaming for attention simultaneously. Security teams today face thousands of alerts daily, and the overwhelming majority are false positives or low-priority noise. Meanwhile, the real threats slip through because analysts are burned out from chasing shadows.

What convinced me we needed something fundamentally different wasn't just the volume, it was watching talented security professionals spend the vast majority of their time on repetitive grunt work: correlating alerts, tracking down asset owners, manually enriching context, compiling compliance evidence. We built incredible detection systems but forgot that humans can't scale the way alerts do. The industry needed something that doesn't just automate tasks but actually understands the entire security program end-to-end, reasons over context, and works alongside humans as a genuine teammate rather than another dashboard to check.

Cybercrime is projected to hit $10.5 trillion, and the industry faces a 4.8 million talent gap, with burnout at an all-time high. From your perspective, what is fundamentally broken in the current security model?

The broken part is simple: we're solving a capacity problem with a technology problem, and it's not working. Every vendor sells us more tools, more automation, more "intelligence," but what we've actually built is a fragmented ecosystem where each tool operates in its own silo, generating its own alerts, requiring its own expertise. Security teams now manage an average of 45+ different security tools, yet breaches still take 258 days to identify and contain.

The result? Security teams aren't short on data; they're short on time and context. An alert from your SIEM means nothing without understanding the asset it's flagged, the vulnerability scanner results, the identity permissions, the business criticality, and whether it's even relevant to your threat model. That manual correlation work is where teams lose the battle. We've optimized for detection but completely underinvested in operational capacity. The current model assumes unlimited human attention span and infinite working hours—both of which we know don't exist.

Do you believe the security talent crisis is solvable—or do we need to redesign the way cybersecurity work is done?

Both, but redesign comes first. We can't hire our way out of this. Even if we magically filled all 4.8 million open roles tomorrow, we'd still be drowning because the work itself is fundamentally structured wrong. The talent crisis

is a symptom, not the disease.

The real shift needs to happen in how we architect security operations. Instead of expecting humans to be the connective tissue between disparate tools, we need systems that handle the operational heavy lifting - the triage, the enrichment, the correlation, the evidence collection - so analysts can focus on judgment, strategy, and response decisions. Think about it: most security work today is about gathering context and making sense of noise. That's exactly what AI-native systems excel at. When we built DST, we didn't ask 'How do we help analysts work faster?' We asked 'what if analysts never had to do this work at all? We don't need more people doing repetitive tasks; we need to redesign security work so that humans do what humans do best, and that is to make critical decisions, while intelligent systems handle everything else.

? How would you describe DST to a CISO who has already spent millions on security tools and platforms?

DST isn't another tool you're adding to the stack. It's the teammate that finally makes your existing stack work together. You've already invested heavily in SIEM, EDR, vulnerability scanners, and compliance platforms, all best-in-class. But they're generating more alerts and data than your team can possibly process. That's not a failure of the tools; it's a failure of coordination.

A Digital Security Teammate integrates across those 200+ platforms you already own. It continuously triages alerts, correlates them with your actual environment, including your assets, vulnerabilities, identities, configurations, and surfaces only what matters with full business context. Instead of your analysts switching between ten consoles to understand one alert, the DST does that work automatically and presents them with actionable intelligence. You're not replacing anything; you're adding the operational layer that unifies everything. In practical terms, teams see 60% less noise, 70% faster detection, and get back roughly 2,000 analyst hours annually. It's not about new capabilities, it's about unlocking the value of what you've already bought.

Think of it this way: you've built a Formula 1 car with those tools, but your team is still changing tires with a hand wrench. DST is the pit crew that makes it all work at speed.

? What is the AI architecture behind DST, and how is it engineered for complex, multi-system security environments?

DST is AI-native from the ground up, not AI bolted onto legacy architecture. The core differentiator is our semantic data layer combined with a reasoning engine built specifically for security operations.

At the foundation, we built a knowledge graph that continuously maps your entire environment: every asset, workload, identity, configuration, SaaS app, and vulnerability. That's not static inventory; it's dynamic context that updates in real-time. On top of that sits our reasoning layer, which uses ML-based classification and contextual analysis to understand relationships - how alerts connect to assets, how vulnerabilities chain into attack paths, how permissions drift creates risk.

The architecture is designed to handle the complexity of multi-cloud, hybrid environments where data lives across AWS, Azure, GCP, on-premise systems, and 200+ security tools. We don't aggregate data and hope for the best; we semantically understand it. That means when an alert fires, DST doesn't just see

"high-severity vulnerability" — it sees the affected asset, its business criticality, who owns it, what it connects to, whether it's internet-facing, and what the actual exploit path looks like. That's the difference between automation and intelligence. We built the entire system, including the architecture, UX, and integration layer, to operate as a collaborative teammate, not a black-box agent.

? Many CISOs fear AI becoming a new attack surface—how does Secure.com secure the AI that secures everything else?

That's the right question to ask, and it's exactly why we designed DST with transparency and human-in-the-loop control as foundational principles, not afterthoughts.

First, every action DST takes is fully auditable. There's no black box. The system shows its reasoning, the evidence it collected, and the decision path it followed. If DST recommends remediation, you see exactly why—what triggered it, what context informed it, and what the expected outcome is. Second, we built explicit approval workflows. High-impact actions require human confirmation. DST can handle the grunt work autonomously, but it doesn't make unilateral decisions about critical infrastructure.

On the security front, DST operates within your existing identity and access controls. It doesn't bypass your governance; it respects it. We also align with regulatory frameworks, such as SOC 2, ISO 27001, SAMA, NCA ECC, specifically because we know CISOs need compliance guarantees, not just performance promises. The architecture is designed so that if DST itself were compromised, it can't escalate privileges or execute arbitrary code. It operates with least-privilege principles and is subject to the same monitoring and controls as any other security tool in your environment. We secure AI the same way we secure everything else: through defense-in-depth, transparency, and accountability.

Guarding the **path**

John Hathaway, VP Sales – META & APAC at BeyondTrust, outlines three common identity attack vectors and how to correct them.

We all know that neighbor who is security-conscious enough to change the locks when they moved in but left a key under a flowerpot on the porch. When it comes to identity security, we often see similar issues where our vulnerabilities hide in plain sight. So, as the United Arab Emirates (UAE) speeds its way through successive economic successes, have its businesses considered all possible Paths to Privilege in their IT systems? For we live in a world where our cyber adversaries no longer hack in; they log in.

The problem is identities. According to the Huntress 2025 Managed ITDR Report, 67% of organisations have seen identity-related incidents increase in just the past three years. These findings are supported by research from Check Point, which found that credential theft has surged by a staggering 160% in 2025 and now accounts for 20% of all data breaches.

Organisations work hard to implement robust security policies, but hidden misconfigurations in our identity infrastructure often leave the metaphorical key under the mat. These misconfigurations open up Paths to Privilege that mean a seemingly harmless identity belonging to a summer intern might suddenly have the ability to become a Global Administrator.

As an attacker, why bother with all the trouble of finding a zero-day exploit and creating complex malware code to remain undetected when one compromised identity with a path to privilege can get you everything you want. Identity misconfigurations are the new malware.

While organisations think in lists of privileges assigned to individuals within siloed systems, their attackers think in graphs of connected identities across systems. Attackers can exploit complex nested group memberships and trust relationships. They can target infrastructure weaknesses. They go after misconfigurations. This holistic view makes it easier for them to move laterally and elevate privileges to achieve their objectives.

Let's take a look at three real world misconfigurations that attackers are actively exploiting in the wild, and how defenders can stop them:

1. Target the infrastructure not the accounts

Stealing domain admin account passwords is hard work, especially as many organisations have placed good controls around these high-risk accounts. Instead, attackers will target misconfigurations in Active Directory Certificate Services (ADCS) that allow any domain user to issue a certificate allowing them to authenticate as a domain admin. With this access-all-areas pass in hand, the attacker can bypass even a well-implemented Privileged Access Management (PAM) solution.

Organisations often overlook the necessity to monitor the

John Hathaway
VP Sales – META & APAC
BeyondTrust

granting of privileges as strictly as they monitor the privileged accounts themselves. They should regularly audit certificate templates and ensure only authorised users can request certificates for privileged accounts.

2. Gaming the helpdesk

If the threat actor can compromise a helpdesk identity in, say, Entra ID, they can reset passwords, including global admin passwords, and add themselves to highly privileged groups. After that, they will have unlimited access to the environment. To stop this, organisations must have full visibility of not just who has a privileged account, but a complete map of who can grant privileges or indirectly elevate privileges now and in the future. It is critical that indirect privilege escalation paths are remediated, and that just-in-time access is put in place for tier-0 actions like password resets.

3. Introducing a rogue identity provider

If a threat actor can introduce a rogue identity provider (IdP) into the environment, they may be able to gain persistent access to other identities in the estate, along with all its privileges.

To counter this threat, security teams must watch for high-risk changes within the identity infrastructure (IdPs, MFA, and federated settings), paying particular attention to privileged accounts. Just like how any endpoint malware may be accompanied by a rootkit designed to enable persistence. Any compromised identity could be part of a bigger issue, so look beyond the account to entire identity and any infrastructure changes that have the potential to grant persistent access.

Mind the gaps

To thwart the threat actor, we need to reduce our identity attack surface, and in order to do this we must uncover the Paths to Privilege within our environments. Organisations must go beyond siloed views of directly granted privileges and think about the ways privileges can be directly or indirectly accessed. A unified identity-centric approach is a reliable way to uncover indirect paths to privilege and the risk behind each identity.

As identity ecosystems expand, occasional privilege access audits will no longer be sufficient. Enterprises must continuously be on the lookout for high-risk changes across their entire identity attack surface, and they must understand what the potential impact of compromise is for each identity. Enforcing the principle of least privilege at the identity level is important to break down silos so least privilege can be applied universally. Remember that the most privileged identities may not be who you think they are, they could be non-human identities or even human identities missing vital MFA or conditional access policies.

We should never make life easy for our assailants. No UAE business wants to make headlines for being the next high-profile target of a cyber-attack. Shaping our environment correctly and ensuring there are no metaphorical keys left under figurative flowerpots involves thinking about all our Paths to Privilege. With due diligence we can rid ourselves of the new malware: identity misconfiguration.

Risk in **focus**

Hadi Jaafarawi, Regional VP, Middle East and Africa, Qualys, shares four cybersecurity trends that will shape risk management in the UAE in 2026.

The United Arab Emirates' cybersecurity market continued its ascendency in 2025 to reach total revenue of some US$820 million, and estimates suggest growth of more than 11% (CAGR) to hit US$1.39 billion by 2030. In a national infrastructure that may be home to more than 223,000 vulnerable digital assets (according to a government report), decision makers must come to terms with their own growing attack surfaces. A burgeoning threat landscape stands before them, equipped with new AI-charged levels of sophistication in attack methods. A glimpse into the coming year may be of help, so let us examine four trends that will shape security postures in 2026.

1. Rise of the ROC

Cybersecurity strategy in the region will continue its shift towards a risk-based view. The modeling of attack paths and the crafting of risk-prioritized operations will take center stage as CISOs embrace the Risk Operations Center (ROC). While asset inventories are important, 2026 will be the year when security teams finally get to grips with risk – defining it, putting it in the proper business context, and using new risk-based metrics to better focus budgets. It will be a new age of more precise triage, less white noise, more intelligently managed resources, and more timely intervention.

2. Dialing down the noise

Between the three T's of telemetry (the data gathered by security apparatuses), tools, and technology (the combination of legacy and emerging solutions), CISOs are overwhelmed. Too many tools deliver too little actionable telemetry, and technologies like AI muddy the internal waters – including giving rise to more high-risk shadow IT – while providing additional options for cyber adversaries. Asset registers alone will not solve the problem of IT sprawl. Modern solutions must be able to show how assets and the risks they pose interact with business value. Only then can organizations approach cybersecurity investments with clear eyes.

3. AI's hidden truths exposed

The UAE is well known for its AI success story. But even as we congratulate ourselves on investments well made, we should be very clear on where the responsibility lies for derisking AI – from LLMs to autonomous (and, at times, anonymous) AI agents. In some circles we hear suggestions of using AI to derisk AI, but what will we use to derisk the derisker? In other words, we run the risk of getting drawn into an infinite risk escalation cycle where the more we try to derisk, the more risk we end up adding.

Before jumping on the bandwagon, weigh the business benefits and risks of AI adoption and compare that to not adopting it. Are we better or worse off? Just because a competitor is applying AI to a problem, it doesn't necessarily mean a measurable

Hadi Jaafarawi
Regional VP, Middle East and Africa, Qualys

business advantage will be gained by following their example. Comparing two decision paths is Risk Management 101. By focusing on business impact and financial implications, we can avoid AI becoming the default solution to every corporate challenge. Prioritize revenue-generating business units and consider how an AI system there could be misused by attackers. If the potential damage outweighs the gains, AI may be better directed towards cost-saving measures elsewhere.

4. Cyber insurance revisited

As of October 2025, analysts valued the UAE cyber-insurance market at US$70 million and there is every reason to believe that market hardening conditions will prevail in 2026, where underwriting is more selective and premiums are higher. Federal Decree-Law No. 34 of 2021 on Combating Rumors and Cybercrimes directs nationally based organizations to take cybersecurity seriously and implement measures on data protection and risk mitigation, but also to comply with regulatory requirements on incident reporting. Since the same requirements apply when applying for cyber insurance, 2026 will be a year of tighter security controls in line with both regulators and insurers.

What is less clear is how the market will view the likelihood of some catastrophic cyber event such as a Web infrastructure outage or a supply-chain compromise or even a mass ransomware campaign that compromises many insured parties at once. However, the UAE's recent history in cyber resilience may also play a role in deciding future premiums.

As the 2026 cyber-insurance market takes shape, there will be opportunities for CISOs to collaborate with colleagues such as the CFO to integrate insurance into the organization's broader risk-management strategy. The challenge will be effectively balancing risk transfer (insurance) and risk mitigation (controls) at a time when security professionals are still figuring out the risk from AI. With the right security posture, companies will be in stronger position to shop around for less costly premiums and stronger policies. One factor likely to differentiate organizations as lower-risk prospects is their use of the right risk platforms – those that provide better visibility into controls and exposure.

New year, new world

As businesses look to protect what matters most, their decision makers must remember that they are entering an era of risk-first cybersecurity. This new world of 'riskonomics' comes with a steep learning curve but offers new opportunities for implanting futureproof capabilities. Given the complexity brought about by new AI technologies, enterprises need to be supported by a strong ROC and a new attitude to risk management that will see it through the coming year and into a brighter future.

The cloud security **illusion**

Hussam Sidani, Vice President for the Middle East and North Africa at OPSWAT, explains why tools without strategy leave enterprises exposed.

Many businesses approach cloud security as a sequence of tasks. Following industry best practices, the latest threat reports, and perhaps even advice from their peers, IT teams go about deploying access controls, encrypting data, implementing monitoring tools, and responding to alerts. Putting all these measures in place is no small task. So, it's only natural that with such robust defences there's a tendency to assume the environment is secure.

The problem is that the cloud never stops changing. Along with every new integration, application, or API come new vulnerabilities. As a result, what is considered secure today can become a weakness tomorrow. Misconfigurations, insecure interfaces, shadow IT, and zero-day exploits are now as common as traditional attack vectors like DDoS or ransomware. In this environment, security cannot be static. It must evolve continuously, with visibility and vigilance at its core.

The Reactive Trap in Cloud Security

Cloud environments are dynamic by design. Workloads scale up and down automatically, applications are updated continuously, and third-party integrations proliferate at speed. Each of these changes creates potential exposure. According to IBM's Cost of a Data Breach Report 2024, 82% of data breaches involve cloud environments, with misconfigurations ranking among the top causes.

This underscores a critical truth: cloud security cannot rely solely on perimeter defences or periodic audits. It requires continuous assessment, proactive remediation, and a clear understanding of how risks evolve over time. The most effective way to achieve this is through a structured Cloud Vulnerability Management (CVM) strategy.

Building a Cloud Vulnerability Management Framework

A comprehensive CVM programme brings together visibility, prioritisation, and remediation in a continuous loop. The following components form the foundation of a proactive approach.

Cloud Vulnerability Assessment

Cloud infrastructure is fluid. New services and configurations are introduced almost daily, and each carries the potential for error or exposure. Regular vulnerability assessments help identify weaknesses before they are exploited, but they must also account for operational realities. Some vulnerabilities cannot be patched immediately without disrupting business continuity. In such cases, structured exception management is vital, documenting the risk, isolating affected systems, and applying compensating controls until a permanent fix can be implemented.

Cloud Security Posture Management (CSPM)

CSPM provides the visibility organisations need to understand

Hussam Sidani
Vice President for the Middle East and North Africa
OPSWAT

their risk exposure at an architectural level. It continuously scans for misconfigurations, policy violations, and excessive permissions across cloud environments. Issues such as unencrypted storage, exposed databases, or overly broad IAM roles are among the most common causes of data leaks. By automating compliance checks against frameworks such as CIS, PCI DSS, and GDPR, the programme ensures that the security posture remains aligned with ever evolving regulatory requirements.

Cloud-Native Application Protection Platforms (CNAPP)

As workloads become more distributed across containers, virtual machines, and serverless architectures, traditional security tools struggle to maintain consistent visibility. CNAPP solutions unify multiple protection layers including CSPM, Cloud Workload Protection (CWPP), and vulnerability management within a single framework. This holistic view enables security teams to monitor risks throughout the application lifecycle, from development to runtime. The result is earlier detection of potential threats and stronger alignment between DevOps and security teams.

Access Controls and Multi-Factor Authentication

Identity remains one of the most exploited weaknesses in cloud environments. Implementing robust access controls ensures that only authorised users and systems can reach specific resources and only to the extent necessary. Regular privilege reviews, separation of duties, and granular access policies help limit lateral movement in the event of a compromise. Multi-Factor Authentication (MFA) further strengthens this layer by requiring multiple forms of verification. Many regulatory frameworks, including ISO 27001 and PCI DSS, now mandate MFA for privileged accounts, reflecting its importance in preventing credential-based attacks.

The Strategic Advantage of Continuous Vigilance

Adopting CVM is not simply about compliance or technical hygiene. It represents a shift in mindset. Mature organisations treat vulnerability management as an ongoing discipline rather than a series of isolated projects. They embed assessment and remediation processes across the full lifecycle of cloud operations, ensuring that every change in the environment is accompanied by a reassessment of risk.

This continuous approach delivers strategic advantages. It improves resilience by reducing the attack surface before adversaries can exploit it. It enhances operational confidence by giving teams visibility into where the most significant risks lie. And, critically, it allows security functions to align more closely with business objectives enabling innovation without compromising control.

Staying Ahead of a Moving Target

Cloud security is not a destination; it is a moving target. The pace of innovation ensures that new vulnerabilities will continue to emerge as fast as old ones are resolved. Cloud Vulnerability Management offers the framework to counter this. By combining visibility, prioritisation, and remediation into a unified strategy, it transforms cloud security from a reactive necessity into a proactive advantage.

How to solve the **performance-security paradox**

CIOs can overcome the performance/security trade-off by unifying networking and security, embedding protection by design and leveraging AI to ensure speed, safety and compliance, writes John Whittle, chief operating officer at Fortinet.

For years, CIOs have been asked to do the impossible: make the business run faster and safer at the same time – while also reducing spending.

Post-pandemic cost discipline has returned, regulators have expanded the scope of critical operations and the C-suite increasingly views technology as the execution engine of strategy. Meanwhile, the cloud has splintered under sovereignty and in-country data requirements. If the job of the CIO was ever a balancing act, today it's a full-blown acrobatics routine.

And yet, the paradox is solvable. Leaders must stop treating performance and security as rival objectives and start designing architectures where they are the same motion.

"Historically, the CIO's primary mandate was performance," says John Whittle, chief operating officer at Fortinet. "Security came second. But that order has flipped. The threat landscape has become far more sophisticated, effectively jumping to a whole new level. The stakes are higher, and vthe board is watching, with resilience now a core expectation."

Cybercrime is a business and, increasingly, a geopolitical weapon, emphasises Whittle. "You can stop ahospital as effectively as you can stop a factory line."

Collapse the stack – or be crushed by it

Complexity is the quiet killer of both performance and security. Tool sprawl fragments policies, duplicates agents and creates expensive gaps. To address this problem, firms would be wise to pursue a platform approach that converges networking and security under a single operating system, policy model and telemetry fabric.

At Fortinet, this is called a secure-by-design approach. "Fortinet has led converging networking and security for 25 years. We see network and security as one discipline," says Whittle. "Treating them as one enables organisations to provide security and networking without compromising performance or resilience, and to more efficiently detect, analyse and respond from a single dashboard.

Otherwise, you're doing manual correlation across logs and consoles and hoping to be fast enough." Simple but powerful correlations, such as edge CPU spikes combined with suspicious encryption behaviour, can signal ransomware in motion. "The point isn't a clever rule. It's that you can only correlate at speed if you see the whole," he explains.

This is where the performance/security trade-off starts to disappear. When

protection is built into the way people and applications connect, systems

don't just stay safer – they run faster.

A single, consistent set of

John Whittle
Chief Operating Officer
Fortinet

policies means fewer gaps and faster change, while a

shared technology backbone makes integration a natural state, not an endless IT project.

SASE, without the sovereignty hangover

Secure-access service edge (SASE) was a breakthrough because it fused SD-WAN connectivity – the backbone of modern enterprise networks – with security. "As you connect, you protect," says Whittle. "You don't bolt security on later as an afterthought."

But SASE's traditional reliance on vendor-cloud points of presence can hit sovereignty and data-residency limits. The new move is sovereign SASE: delivering the full SASE stack in customer-controlled environments so traffic and telemetry never leave approved boundaries, while keeping the unified policy, identity and zero-trust model.

This means CIOs don't have to choose between user experience and compliance; they can require both in the design. The litmus test for suppliers is simple: can they enforce one policy everywhere – the office, home offices, factories, different branches, the public cloud and private data centres and keep inspection and storage where the law (and risk appetite) demands?

If SASE is where performance and security converge for users and edges, cloud-native application-protection platforms (CNAPP) are where they converge for modern software. Over the past decade, cloud security has fractured into discrete tools: posture

management, workload protection, entitlement governance, container scanning and infrastructure as code (IaC) checks. CNAPP consolidates these into a single data model from code to runtime, turning a noisy audit exercise into an engineering workflow.

"It's not about how many findings you have. It's about which ones matter to business risk and resilience and how fast you can fix them," says Whittle. Fortinet's approach looks at both the application behaviour (Is it doing something that violates policy?) and

the underlying resources (Are the components and links themselves introducing risk?) to provide a complete view of exposure and ensure nothing slips through the gaps.

People, platforms and the paradox

Elsewhere, operational resilience has become a legal mandate across sectors,

expanding what counts as "critical". That pushes architecture decisions into the

boardroom. Where is inspection performed? Where are logs retained? Who can access telemetry? Can you prove segmentation and policy consistency across facilities, partners and clouds?

Here, convergence pays a second dividend: compliance by construction. If your platform maintains one policy ontology and one audit trail, evidencing obligations becomes a by-product of the way you run, not a scramble after the fact.

At the same time, no platform strategy works without people. Skills shortages are a structural risk, and AI has sharpened both the threat and the opportunity. Attackers use AI to mimic language and context convincingly, which makes it critical for organisations to provide AI for security while ensuring security for AI systems themselves.

"AI can already deceive human reflexes and the equivalent defences in hardware and software," Whittle says, "while defenders can use AI to speed triage, summarise alerts and harden code earlier.

Speed or safety?

No longer a compromise CIOs should be pragmatic here: choose platforms your team can operate, then invest in targeted upskilling that exploits embedded automation and AI safely. As Whittle puts it: "You can have the best cyber strategy in the world, but if you don't have the people to execute, you're still at risk."

"The CIO role is changing," adds Whittle. "New legal, geopolitical and operational dimensions are coming their way. But they don't have to choose between speed and safety," he says. "Fortinet was founded on that premise, integrating both and never having to jeopardise one over the other. See the network and security converged as one, keep a holistic view and execute from a single fabric. That's how you stay fast and secure."

The performance/security paradox is no longer a zero-sum game. By unifying networking and security, CIOs can embed protection directly into design. AI-enabled tools and skilled teams then make speed, safety and compliance achievable at once. The key is to treat performance and security as two sides of the same coin, notcompeting priorities.

Cybersecurity in 2026: The year of Intelligent Resilience

"In 2026, cybersecurity is not just about defense - it's about staying one step ahead."

As we step into 2026, the cybersecurity ecosystem continues to evolve at an unprecedented pace. The rise of AI, cloud-native infrastructures, and interconnected industrial systems is creating both new opportunities and new risks. For businesses, governments, and individuals alike, staying ahead of cyber threats has never been more critical.

Rehisha Pallikkathodi Erathali
Assistant Editor, GEC

One of the defining trends this year is the shift from reactive security to intelligent resilience. Cyber leaders are no longer just protecting networks - they are building systems that anticipate, adapt, and respond in real time. AI-driven threat detection, automated incident response, and predictive analytics are moving from experimental tools to essential components of enterprise security.

Another key focus for 2026 is cyber-physical security. As operational technology (OT) and Internet of Things (IoT) networks grow, the lines between physical and digital security blur. Protecting industrial systems, smart cities, and critical infrastructure requires a combination of AI intelligence, endpoint visibility, and robust monitoring - ensuring safety without slowing down innovation.

Data security remains the backbone of this evolution. With AI initiatives scaling across enterprises, the importance of secure, resilient, and well-governed data cannot be overstated. Companies are increasingly adopting integrated solutions that combine data protection, governance, and compliance into a unified command centre, giving CIOs and CISOs the tools to power AI securely.

For cybersecurity professionals, 2026 is a year to think beyond threats and embrace transformation. It's about cultivating a culture where security is woven into every layer of technology and business strategy, and where innovation and protection move hand in hand.

As we begin the year, one thing is clear: cybersecurity is no longer just a safeguard - it's a strategic enabler. The organisations that succeed will be those that leverage intelligence, foresight, and resilience to stay one step ahead in an ever-changing digital world.

> "For cybersecurity professionals, 2026 is a year to think beyond threats and embrace transformation."

GEC Global Enterprise Connect

CLOUD SUMMIT 2026

DUBAI KNOWLEDGE PARK, UAE
05 FEB

VOCO RIYADH, KSA
12 FEB

KENYA
19 AUG

PHILIPPINES
26 OCT

INDONESIA
27 OCT

MALAYSIA
29 OCT

#cloudsummit